

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-63084

(P2002-63084A)

(43) 公開日 平成14年2月28日 (2002.2.28)

(51) Int.Cl. ⁷	識別記号	F I	テームト* (参考)
G 0 6 F 13/00	3 5 1	G 0 6 F 13/00	3 5 1 Z 5 B 0 8 9
H 0 4 L 12/66		H 0 4 L 11/20	B 5 K 0 3 0
12/56			1 0 2 A

審査請求 有 請求項の数35 O L (全 28 頁)

(21) 出願番号 特願2000-249724(P2000-249724)

(22) 出願日 平成12年8月21日 (2000.8.21)

(71) 出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72) 発明者 楯岡 正道

東京都青梅市末広町2丁目9番地 株式会
社東芝青梅工場内

(74) 代理人 100058479

弁理士 鈴江 武彦 (外6名)

Fターム(参考) 5B089 GA04 GB01 HA04 KA17 KB13

5K030 GA15 HA08 JA05 KA03 KA13

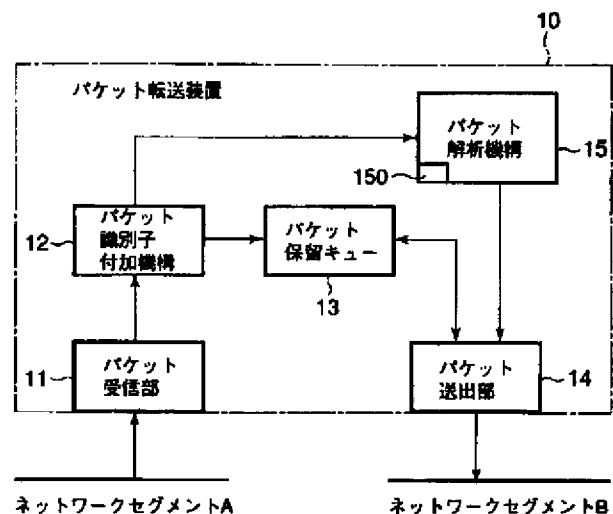
KX13 KX24 KX30 LCO1 LC15

(54) 【発明の名称】 パケット転送装置、パケット転送方法、及びそのプログラムが格納された記憶媒体

(57) 【要約】

【課題】 本発明は、パケットを転送するか否かの判断を行なうための設定を利用者が行なうことなく、不正アクセスに関わるパケットを通過させないパケット転送装置を実現することができるパケット転送装置、パケット転送方法、及びそのプログラムを格納した記憶媒体を提供することを課題とする。

【解決手段】 パケット識別子付加機構12からパケットを渡されたパケット送出機構15は、当該パケットを予め設定された情報に基づいて送出し、当該パケットが不正アクセスに関わるか否かを判定する。



【特許請求の範囲】

【請求項1】 複数のネットワークセグメントの間に設けられ、ネットワークセグメント相互間で転送されるパケットを監視するパケット転送装置であって、第1のネットワークセグメントを介して受信した受信パケットを第2のネットワークセグメントに送出する際に、予め設定された条件をもとに、前記受信パケットの情報に、前記第2のネットワークセグメントに接続された装置のソフトウェアに対し誤動作させる要因を含んでいるか否かを解析するパケット解析手段と、前記解析手段によって前記誤動作させる要因を含んだ情報をもつ不正パケットであることを判定した際に、当該不正パケットを破棄し、正常なパケットと判定した受信パケットのみを前記第2のネットワークセグメントに送出する手段とを具備してなることを特徴とするパケット転送装置。

【請求項2】 少なくとも第1及び第2のネットワークセグメントに接続され、前記第1及び第2のネットワークセグメント相互の間で転送されるパケットに不正アクセスを起こすパケットが含まれる場合、その不正パケットを排除するパケット転送装置に於いて、前記第1のネットワークセグメントからのパケットを受信する受信手段と、前記受信手段で受信した受信パケットに識別子を付加する識別子付加手段と、前記識別子が付加された前記受信パケットを一時保留するパケット保留キューと、前記受信パケットが予め設定した既知の誤動作条件を含む不正アクセスのパケットであるか否かを判定し、不正アクセスに関わるパケットで無いことを判定した際に、当該受信パケットの識別子を出力するパケット解析手段と、前記パケット解析手段より出力された前記識別子を受信し、前記パケット保留キューから受信した前記識別子を持つ受信パケットを取り出し、前記第2のネットワークセグメントへ送出する送出手段とを具備することを特徴とするパケット転送装置。

【請求項3】 少なくとも3つ以上のネットワークセグメントに接続され、複数の前記ネットワークセグメント間で転送されるパケットに不正アクセスを起こすパケットが含まれる場合、その不正パケットを排除するパケット転送装置に於いて、前記ネットワークセグメントからのパケットを受信する受信手段と、前記受信手段で受信した受信パケットに識別子を付加する識別子付加手段と、前記識別子が付加された前記受信パケットを一時保留するパケット保留キューと、

前記受信パケットが予め設定した既知の誤動作条件を含む不正アクセスのパケットであることを判定した際に、当該受信パケットの識別子を出力するパケット解析手段と、前記パケット解析手段より出力された前記識別子を受信し、前記パケット保留キューから受信した前記識別子を持つ受信パケットを取り出し、前記第2のネットワークセグメントへ送出する送出手段とを具備することを特徴とするパケット転送装置。

アクセスに関わるパケットで無いことを判定した際に、当該受信パケットの識別子を出力するパケット解析手段と、前記パケット解析手段より出力された前記識別子を受信し、前記パケット保留キューから受信した前記識別子を持つ受信パケットを取り出し、当該受信パケットに含まれる宛先MACアドレスから、送出すべきネットワークセグメントを判定する送出セグメント判定手段と、前記送出セグメント判定手段によって判定されたネットワークセグメントへ当該受信パケットを送出する1つ又は複数の送出手段とを具備することを特徴とするパケット転送装置。

【請求項4】 少なくとも3つ以上のネットワークセグメントに接続され、複数の前記ネットワークセグメント間で転送されるパケットに不正アクセスを起こすパケットが含まれる場合、その不正パケットを排除するパケット転送装置に於いて、前記ネットワークセグメントからのパケットを受信する受信手段と、前記受信手段で受信した受信パケットに識別子を付加する識別子付加手段と、前記識別子が付加された前記受信パケットを送出先のネットワークセグメント毎に一時保留する複数のパケット保留キューと、前記識別子が付加された前記受信パケットに含まれる宛先MACアドレスから前記受信パケットの送出先ネットワークセグメントを判定し、当該ネットワークセグメントに対応する前記パケット保留キューに前記識別子が付加されたパケットを送出する送出セグメント判定手段と、前記受信パケットが予め設定した既知の誤動作条件を含む不正アクセスのパケットであるか否かを判定し、不正アクセスに関わるパケットで無いことを判定した際に、当該受信パケットの前記識別子を出力するパケット解析手段と、前記パケット保留キューに対応して設けられる複数の送出手段であって、前記パケット解析手段より出力された前記識別子を受信し、前記識別子を持つ受信パケットを保留している1つ又は複数の前記パケット保留キューから当該受信パケットを取り出し、対応付けられた前記ネットワークセグメントへ送出する送出手段とを具備することを特徴とするパケット転送装置。

【請求項5】 前記パケット解析手段は、過去に受信した不正アクセスに関わるパケットに含まれる文字列を記憶したデータベースを具備することを特徴とする請求項1または2または3または4記載のパケット転送装置。

【請求項6】 前記パケット転送装置に於いて、更に、前記パケット解析手段により不正アクセスに関わるパケットが検出された場合に、その不正パケットの識別子を出力するパケット解析手段と、前記パケット解析手段より出力された前記識別子を受信し、前記パケット保留キューから受信した前記識別子を持つ受信パケットを取り出し、前記第2のネットワークセグメントへ送出する送出手段とを具備することを特徴とするパケット転送装置。

かを含む詳細情報を取得して保持する不正アクセス履歴保持手段と、

前記不正アクセス履歴保持手段が保持する不正アクセス履歴を表示する不正アクセス履歴表示手段とを具備することを特徴とする請求項1または2または3または4記載の packets 転送装置。

【請求項7】 前記 packets 転送装置に於いて、更に、前記 packets 解析手段によって不正 packets でないと判定された送出済み packets を保持する送出済み packets 保持手段を設け、

前記 packets 解析手段は不正 packets の解析時に、前記送出済み packets 保持手段に保持された前記送出済み packets を参照することを特徴とする請求項1または2または3または4記載の packets 転送装置。

【請求項8】 前記 packets 解析手段は、前記受信 packets のヘッダ部のオプション、若しくはパラメータの組み合わせが、予め設定された既知の条件を満たしているか否かを判定する手段、

前記受信 packets が搬送しているデータの長さ、若しくはデータが指定するパラメータの組み合わせが、予め設定された既知の条件を満たしているか否かを判定する手段、

packets 相互のデータ構造、若しくはデータ内容が、予め設定された既知の条件を満たしているか否かを判定する手段の少なくとも一つの手段により、不正アクセスに関わる packets であるか否かを判定することを特徴とする請求項1または2または3または4記載の packets 転送装置。

【請求項9】 前記 packets 解析手段は、前記識別子が付加された受信 packets を格納する packets 格納手段と、

不正アクセスの packets に含まれる文字列を一部に内蔵する packets 解析プログラムが格納されるプログラム格納手段と、

前記 packets 解析プログラムに基づき、前記 packets 格納手段に格納された受信 packets について、既知の誤動作条件を含む不正アクセスの packets であるか否かを判定し、不正アクセスに関わる packets で無いことを判定した際に、当該受信 packets の識別子を出力するプログラム実行手段とを具備することを特徴とする請求項1または2または3または4記載の packets 転送装置。

【請求項10】 前記 packets 転送装置は、更に、前記プログラム格納手段に格納された前記 packets 解析プログラムを更新する解析プログラム更新手段を具備することを特徴とする請求項9記載の packets 転送装置。

【請求項11】 前記解析プログラム更新手段は、シリアルインタフェース、若しくはネットワークインタフェースでなる通信インタフェースと、

前記通信インタフェースを介して受信したデータから

ることを識別する解析プログラム更新指示形式の識別手段とを具備し、

前記解析プログラム更新指示形式の識別手段が前記解析プログラム更新指示であると識別したデータをもとに、前記 packets 解析プログラムをロード、若しくは更新することを特徴とする請求項10記載の packets 転送装置。

【請求項12】 前記解析プログラム更新手段は、前記受信手段で受信した packets から、前記 packets 解析プログラムの更新指示を示す特定の形式を満たしているデータであることを識別する解析プログラム更新指示形式の識別手段を具備し、

前記解析プログラム更新指示形式の識別手段が前記解析プログラム更新指示であると識別した受信 packets のデータをもとに、前記 packets 解析プログラムをロードし、若しくは更新することを特徴とする請求項10記載の packets 転送装置。

【請求項13】 前記解析プログラム更新指示形式の識別手段は、

前記 packets 内のデータ、若しくは前記シリアルインタフェースを介して入力されたデータ、若しくは前記ネットワークインタフェースを介して入力されたデータから、電子署名情報を抽出し、当該電子署名情報が正当な署名であるか否かを判定し、正当であると判定した場合、前記 packets 解析プログラムをロードし、若しくは更新することを特徴とする請求項12記載の packets 転送装置。

【請求項14】 前記 packets 転送装置は、更に、前記 packets 解析手段が不正アクセスに関わる packets であると判定した場合、その不正 packets の存在、構造、形式、受信時刻、送信元等の少なくともいずれかをを含む詳細情報を他の装置に通知する装置内情報通知手段を具備することを特徴とする請求項1または2または3または4記載の packets 転送装置。

【請求項15】 前記 packets 解析プログラムの設定または更新に伴う通信、若しくは不正 packets の前記詳細情報を他の装置に通知する通信である特定通信のみに使用する送信元アドレスを予め設定する通信用アドレス設定手段と、前記通信用アドレス設定手段により設定された通信用アドレスを保持する通信用アドレス保持手段と、

前記特定通信を行わないときは、前記送信元アドレス宛てに送られる packets を破棄し、前記特定通信を行うときのみ、前記送信元アドレス宛ての packets を受信する通信制御手段とを具備してなることを特徴とする請求項10または14記載の packets 転送装置。

【請求項16】 前記 packets 解析プログラムの設定または更新に伴う通信、若しくは不正 packets の前記詳細情報を他の装置に通知する通信である特定通信のために

ットワークセグメントとは異なるネットワークセグメントから過去に受信したパケットの送信元アドレスの1つを選択する通信用アドレス選択手段と、

前記通信用アドレス選択手段で選択された送信元アドレスを宛先としたパケットのうち、当該特定通信に関わるパケットを横奪するパケット横奪手段とを具備することを特徴とする請求項10または14記載のパケット転送装置。

【請求項17】 転送対象であるパケットから前記特定通信の開始指示である特定の形式を満たしているデータであることを識別して、前記特定通信を開始する通信開始指示形式識別手段を具備することを特徴とする請求項15または16記載のパケット転送装置。

【請求項18】 前記通信開始指示形式識別手段は、データ中に含まれている電子署名が正当な署名であるか否かを判定し、正当な署名であると判定した場合のみ当該データを通信開始指示であると識別する電子署名識別手段を具備することを特徴とする請求項17記載のパケット転送装置。

【請求項19】 複数のネットワークセグメントの間に設けられ、ネットワークセグメント相互間で転送されるパケットを監視するパケット転送装置であって、第1のネットワークセグメントより受信した受信パケットを第2のネットワークセグメントに送出する際に、予め設定された条件をもとに、前記受信パケットの情報に、前記第2のネットワークセグメントに接続される装置のソフトウェアに対し誤動作させる要因を含んでいるか否かを判定し、前記誤動作させる要因を含んだ情報をもつ不正パケットであることを判定した際に、当該不正パケットを破棄し、正常なパケットと判定した受信パケットを前記第2のネットワークセグメントに送出することを特徴とするパケット転送方法。

【請求項20】 少なくとも第1及び第2のネットワークセグメントに接続され、前記第1及び第2のネットワークセグメント相互の間で転送されるパケットに不正アクセスを起こすパケットが含まれる場合、その不正パケットを排除するパケット転送方法に於いて、前記第1のネットワークセグメントからのパケットを受信するステップと、前記受信した受信パケットに識別子を付加するステップと、前記識別子が付加された前記受信パケットを一時保留するステップと、前記識別子が付加された前記受信パケットを解析し、不正アクセスに関わるパケットでないことを判定し、判定した正常な受信パケットの前記識別子を出力するステップと、

前記識別子を出力し、前記一時保留されている前記受信パ

ケットを取り出し、前記第2のネットワークセグメントに送出するステップとを具備することを特徴とするパケット転送方法。

【請求項21】 少なくとも3つ以上のネットワークセグメントに接続され、複数の前記ネットワークセグメント間で転送されるパケットに不正アクセスを起こすパケットが含まれる場合、その不正パケットを排除するパケット転送方法に於いて、

前記ネットワークセグメントの一つからパケットを受信するステップと、

前記受信した受信パケットに識別子を付加するステップと、

前記識別子が付加された前記受信パケットを一時保留するステップと、

前記識別子が付加された前記受信パケットを解析し、不正アクセスに関わるパケットでないことを判定し、判定した正常な受信パケットの前記識別子を出力するステップと、

前記識別子を受信し、前記一時保留されている前記受信

パケットの中から、受信した前記識別子を持つ前記受信パケットを取り出し、当該受信パケットに含まれるMACアドレスから送出すべきネットワークセグメントを判定するステップと、

前記判定されたネットワークセグメントに対し、取り出した前記受信パケットを送出するステップとを具備することを特徴とするパケット転送方法。

【請求項22】 少なくとも3つ以上のネットワークセグメントに接続され、複数の前記ネットワークセグメント間で転送されるパケットに不正アクセスを起こすパケットが含まれる場合、その不正パケットを排除するパケット転送方法に於いて、

前記ネットワークセグメントの一つからパケットを受信するステップと、

前記受信した受信パケットに識別子を付加するステップと、

前記識別子が付加された前記受信パケットに含まれる宛先MACアドレスから当該受信パケットの送出先ネットワークセグメントを判定し、前記送出先のネットワークセグメント毎に設けられた一時保留キューに、前記判定に従って前記受信パケットを格納するステップと、

前記識別子が付加された前記受信パケットを解析し、不正アクセスに関わるパケットでないことを判定し、判定した正常な受信パケットの前記識別子を出力するステップと、

前記識別子を受信し、前記一時保留キューの前記受信パケットの中から、受信した前記識別子を持つ前記受信パケットを取り出し、対応するネットワークセグメントに送出するステップとを具備することを特徴とするパケッ

ト転送方法。

に、
不正アクセスに関わるパケットであると判定したパケットの受信時刻、若しくは送信元を少なくとも含む詳細情報を記録するステップと、
当該記録された詳細情報を表示するステップとを有してなる請求項19または20または21または22記載のパケット転送方法。

【請求項24】 前記パケット転送方法に於いて、更に、
前記正常なパケットと判定され、過去に送出済み受信パケットを保持する送出済みパケット保持手段を設け、
前記パケット解析時に、前記パケット保持手段に格納された前記送出済み受信パケットを参照して、不正アクセスに関わるパケットであるか否かの判定を行なうステップを有することを特徴とする請求項19または20または21または22記載のパケット転送方法。

【請求項25】 前記パケット転送方法に於いて、更に、
前記識別子が付加された受信パケットを格納するパケット格納手段と、不正アクセスのパケットに含まれる文字列を一部に内蔵するパケット解析プログラムが格納されるプログラム格納手段と、前記パケット解析プログラムを実行するプログラム実行手段とを設け、
前記受信パケットの解析時に、プログラム実行手段は、前記パケット解析プログラムに基づき、前記パケット格納手段に格納された受信パケットについて、既知の誤動作条件を含む不正アクセスのパケットであるか否かを判定し、不正アクセスに関わるパケットで無いことを判定した際に、当該受信パケットの識別子を出力することを特徴とする請求項20または21または22記載のパケット転送方法。

【請求項26】 前記パケット転送方法に於いて、更に、
シリアルインタフェース、若しくは前記ネットワークインタフェース、若しくは独立したネットワークインタフェースを介して前記パケット解析プログラムの更新指示のデータを受信するステップと、
受信したデータが前記パケット解析プログラムの更新指示を示す特定の形式を満たしていることを識別できた時に、前記パケット解析プログラムを更新するステップとを有してなることを特徴とする請求項25記載のパケット転送方法。

【請求項27】 前記パケット転送方法に於いて、前記パケット解析プログラムの更新指示を示す特定の形式を満たしていることを識別するために、前記受信したデータ中に含まれている電子署名が正当な署名であるか否かを判定することを特徴とする請求項26記載のパケット転送方法。

【請求項28】 前記パケット転送方法に於いて、更に、

不正アクセスに関わるパケットであると判定したパケットの受信時刻、送信元の少なくともいずれかを含む詳細情報を記録するステップと、

当該記録された詳細情報を他の装置に通知するステップとを具備することを特徴とする請求項19または20または21または22記載のパケット転送方法。

【請求項29】 前記パケット転送方法に於いて、更に、
前記パケット解析プログラムの更新に伴う通信や、装置内の情報を他の装置に対して通知する通信などの特定通信を行なう際に使用する送信元アドレスを、予め設定するステップを具備し、
前記特定通信を行なう間のみ、前記送信元アドレス宛のパケットを受信し、
前記特定通信を行なっていない間は、前記送信元アドレス当てのパケットを破棄することを特徴とする請求項26または28記載のパケット転送方法。

【請求項30】 前記パケット転送方法に於いて、更に、
前記パケット解析プログラムの更新に伴う通信や、装置内の情報を他の装置に対して通知する通信などの特定通信を行なう際に使用する送信元アドレスを、送信先ネットワークセグメントとは異なるネットワークセグメントから、過去に受信したパケットの送信元アドレスの一つを、当該通信を行なう際の送信元アドレスとして、予め選択するステップを具備し、
前記特定通信を行なう間のみ、前記送信元アドレス宛ての通信に関わるパケットを横奪し、
前記特定通信を行なっていない間は、前記送信元アドレス宛てのパケットは転送処理を行なうことを特徴とする請求項26または28記載のパケット転送方法。

【請求項31】 前記パケット転送方法に於いて、前記受信パケットが不正アクセスに関わるパケットであると判定する条件は、
前記受信パケットのヘッダフィールドのオプション、若しくはパラメータの組み合わせが、パケット送出先に誤動作を引き起こす可能性があるとして予め設定された既知の条件を満たしているとき、
又は、前記受信パケットが搬送しているデータの長さ、若しくはデータが指定するパラメータの組み合わせが、当該データを処理するソフトウェアに誤動作を引き起こす可能性があるとして予め設定された既知の条件を満たしているとき、
又は、前記受信パケット相互のデータ構造、若しくはデータ内容が、パケット送出先に誤動作を引き起こす可能性があるとして予め設定された既知の条件を満たしているとき、

のいずれかであることを特徴とする請求項19または20または21または22記載のパケット転送方法。

グメント相互の間で転送されるパケットを監視するパケット転送装置に記憶され、
前記ネットワークセグメントの一方からのパケットを受信する機能と、
前記受信した受信パケットに識別子を付加する機能と、
前記識別子が付加された前記受信パケットを一時保留する機能と、
前記識別子が付加された前記受信パケットを解析し、不正アクセスに関わるパケットでないことを判定した際に、当該受信パケットの識別子を出力する機能と、
前記識別子を受信し、前記一時保留されているパケットの中から受信した前記識別子を持つ受信パケットを取り出し、送出先の他方のネットワークセグメントへ送出する機能とを実現するためのプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項33】 少なくとも3つ以上のネットワークセグメント間で転送されるパケットを監視するパケット転送装置に記憶され、
前記ネットワークセグメントの一つからパケットを受信する機能と、
前記受信した受信パケットに識別子を付加する機能と、
前記識別子が付加された前記受信パケットを一時保留する機能と、
前記識別子が付加された前記受信パケットを解析し、不正アクセスに関わるパケットでないことを判定した際に、当該受信パケットの識別子を出力する機能と、
前記識別子を受信し、前記一時保留されている受信パケットの中から受信した前記識別子を持つ受信パケットを取り出し、当該受信パケットに含まれるMACアドレスから送出すべきネットワークセグメントを判定する機能と、
前記判定されたネットワークセグメントへ当該受信パケットを送出する機能とを実現するためのプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項34】 少なくとも3つ以上のネットワークセグメント間で転送されるパケットを監視するパケット転送装置に記憶され、
前記ネットワークセグメントの一つからパケットを受信する機能と、
前記受信した受信パケットに識別子を付加する機能と、
前記識別子が付加された前記受信パケットに含まれるMACアドレスから、送出すべきネットワークセグメントを判定する機能と、
前記識別子が付加された前記受信パケットを、前記判定された送出先ネットワークセグメント毎に分けて一時保留する機能と、
前記識別子が付加された前記受信パケットを解析し、不正アクセスに関わるパケットでないことを判定した際に、当該受信パケットの識別子を出力する機能と、

パケットの中から、受信した前記識別子を持つ受信パケットを取り出し、当該受信パケットを、前記判定された送出先ネットワークセグメントへ送出する機能とを実現するためのプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項35】 前記受信パケットを解析し、不正アクセスに関わるパケットであるか否かを判定する機能を実現するプログラムに、

10 予め設定された既知の条件をもとに、前記受信パケットのヘッダフィールドのオプション、若しくはパラメータの組み合わせが、パケット送出先に誤動作を引き起こす可能性のある不正アクセスに関わるパケットを判定する機能、

予め設定された既知の条件をもとに、前記受信パケットが搬送しているデータの長さ、若しくはデータが指定するパラメータの組み合わせが、当該データを処理するソフトウェアに誤動作を引き起こす可能性のある不正アクセスに関わるパケットを判定する機能、

20 予め設定された既知の条件をもとに、前記受信パケット相互のデータ構造、若しくはデータ内容が、パケット送出先に誤動作を引き起こす可能性のある不正アクセスに関わるパケットを判定する機能、
の少なくとも一つ以上の機能が組み込まれた請求項32または33または34記載のコンピュータ読み取り可能な記憶媒体。

【発明の詳細な説明】

【0001】

30 【発明の属する技術分野】 本発明は、複数のネットワークセグメント相互の間でパケットを転送するパケット転送装置、パケット転送方法、及びそのプログラムが格納された記憶媒体に関する。

【0002】

【従来の技術】 従来、複数のネットワークセグメント相互の間に接続されて、これらセグメント間でパケットを転送するパケット転送装置に於いて、不正アクセスを防止するための、パケットを転送するか否の判断は、利用者がネットワーク若しくは他の設定手段を用いて設定した、宛先/送信元のネットワークアドレスやサービス番号等により行っていた。

40 【0003】 この際の従来のパケット転送装置に於ける不正アクセス防止手段を図2乃至図4を参照して説明する。従来のパケット転送装置の構成例を図2に示している。ここでは、パケット転送装置01の構成要素として、送信元となる一方のネットワークセグメントからのパケットを受信するパケット受信部02、パケット受信部02で受信したパケットをフィルタリング（選定）制御するパケットフィルタ部03、パケットフィルタ部03を通過したパケットを送出先となる他方のネットワークセグメントへ送出するパケット送出部04、不正

クアドレスやサービス番号等を設定するルール設定部05、ルール設定部05で設定されたアドレス等の情報を保持しパケットフィルタ部03が参照するルール保持部06等が設けられる。

【0004】上記構成によるパケット転送装置01を含むネットワークシステムの一構成例を図23に示し、パケット転送装置01のルール保持部06に格納される内容例を図24に示している。

【0005】利用者は、ネットワークを介し、ルール設定部05の機能を用いて、ルール保持部06に、宛先/送信元ネットワークアドレス、サービス番号、転送を許可するか否かの識別情報等を予め設定しておく。

【0006】ここでは上記図22に示す構成のパケット転送装置01を用いて上記図23に示すようなネットワークシステムが構築され、利用者がルール設定部05の機能を用いて図24に示すような設定内容(ルール)が予めルール保持部06に保持しているものとする。

【0007】その状態で、例えば、ネットワークアドレスとして、[192. 168. 1. 12]を持つホストから、[192. 168. 0. 31]を持つホストのH 20 TTPサービスを利用しようとするパケットがパケット受信部02で受信されたとする。

【0008】この受信パケットは、パケットフィルタ部03に送られる。

【0009】パケットフィルタ部03では、ルール保持部06に格納された、予め利用者が設定した図24に示すようなルールを参照する。

【0010】ここでパケットフィルタ部03は、図24に示すルールを参照して、ネットワークアドレスとして、[192. 168. 1. 12]を持つホストから、 30 [192. 168. 0. 31]を持つホストのH TTPサービスを利用するアクセスは許可されていることを判断し、上記パケットをパケット送出部04に送出する。そして、パケット送出部04からネットワークアドレスとして、[192. 168. 0. 31]のアドレスを持つホストへ転送され、通信が完了する。

【0011】また、例えば、ネットワークアドレスとして、[192. 168. 1. 13]を持つホストから、[192. 168. 0. 31]を持つホストのH TTPサービスを利用しようとするパケットがパケット受信部 40 02で受信されたとすると、その受信パケットは、パケットフィルタ部03に送られる。

【0012】パケットフィルタ部03では、ルール保持部06に格納された、利用者が予め設定した図24に示すルールを参照する。

【0013】ここでパケットフィルタ部03は、図24に示すルールを参照すると、ネットワークアドレスとして、[192. 168. 1. 13]を持つホストから、[192. 168. 0. 31]を持つホストのH TTP

を判断する。したがって、このパケットはパケットフィルタ部03によって不正アクセスと判断し破棄され、パケット送出部04からは上記受信したパケットが送出されないこととなる。

【0014】他の宛先/送信元/サービスの各パケットに関しても、上記同様に、図24に示すルール保持部06の内容(ルール)に従って、送出/破棄が行なわれる。

【0015】上述した従来のパケット転送装置に於ける不正アクセス防止手段には、宛先/送信元のMAC(Media Access Control)アドレスや、さらに上位のプロトコルの宛先/送信元アドレスやサービス番号等によって、パケットを転送するか否かを判断するだけでは、転送するように設定されたアドレスやサービス番号を用いた不正アクセスは防止できず、不正アクセスに関わるパケットを通過させないという目的には、不十分であるという問題があった。

【0016】例えば、宛先/送信元MACアドレスや、さらに上位のプロトコルの宛先/送信元アドレスやサービス番号等がすべて正しく設定されていたとしても、その設定された送信元を介して(経由して)不正アクセスと見做されるデータをもつパケットが転送され、当該パケットで搬送されたデータにより、受信側システムのアプリケーション等が侵害されてしまうという、信頼性の問題があった。

【0017】また、パケットを転送するか否かの判断を行なうための宛先/送信元MACアドレスや、さらに上位のプロトコルの宛先/送信元アドレスやサービス番号等の設定は、利用者や設置場所毎に異なるため、パケット転送装置の設置に伴って、設定を行なう必要があったが、この設定は、比較的困難であり、しばしば誤った設定がなされ、不正アクセスを許してしまうという問題もあった。

【0018】また、設定をネットワーク経由で行なうにはIPアドレス等のネットワークアドレスが必要であり、それは、逆に不正アクセスの対象となり得るという問題もあった。

【0019】また、宛先/送信元MACアドレスや、さらに上位のプロトコルの宛先/送信元アドレスやサービス番号等によって、転送しないと判断するパケットが到着したとしても、それが、必ずしも不正アクセスとはいき切れず、したがって、転送しないと判断するパケットが到着したことを何らかの形で表示したとしても、不正アクセスがなされていることの表示とはならないという問題もあった。

【0020】

【発明が解決しようとする課題】上述したように、従来のパケット転送装置に於ける不正アクセス防止手段に於いては、宛先/送信元のMACアドレスや、さらに上位

によって、パケットを転送するか否かを判断するだけでは、転送するように設定されたアドレスやサービス番号を用いた不正アクセスは防止できず、不正アクセスに関わるパケットを通過させないという目的には、不十分であるという問題があった。

【0021】また、パケットを転送するか否かの判断を行なうための宛先/送信元MACアドレスや、さらに上位のプロトコルの宛先/送信元アドレスやサービス番号等の設定は、利用者や設置場所毎に異なるため、パケット転送装置の設置に伴って、設定を行なう必要があったが、この設定は、比較的困難であり、しばしば誤った設定がなされ、不正アクセスを許してしまうという問題もあった。

【0022】また、設定をネットワーク経由で行なうには、IPアドレス等のネットワークアドレスが必要であり、それは、逆に不正アクセスの対象となり得るという問題もあった。

【0023】更に、宛先/送信元MACアドレスや、さらに上位のプロトコルの宛先/送信元アドレスやサービス番号等によって、転送しないと判断するパケットが到着したとしても、それが、必ずしも不正アクセスとはいき切れず、したがって、転送しないと判断するパケットが到着したことを何らかの形で表示したとしても、不正アクセスがなされていることの表示とはならないという問題もあった。

【0024】このように、従来のパケット転送装置に於いては、不正アクセス防止に関して、信頼性の面で種々の問題があるとともに、利用者にかかる作業負担が大きいという問題があった。

【0025】本発明は上記実情に鑑みなされたもので、利用者に大きな作業負担をかけることなく、信頼性の高い不正アクセスの防止機能を実現できるパケット転送装置、パケット転送方法、及びそのプログラムが格納された記憶媒体を提供することを目的とする。

【0026】また本発明は、送信元より転送されたパケット（受信パケット）の内容を送出して不正アクセスに関わるパケットでないことを判定する機能をもつことで、不正アクセスに関わるパケットの転送を確実に防止することのできる、信頼性の高い不正アクセスの防止機能を実現できるパケット転送装置、パケット転送方法、及びそのプログラムが格納された記憶媒体を提供することを目的とする。

【0027】また本発明は、宛先/送信元MACアドレスや、上位のプロトコルの宛先/送信元アドレスや、サービス番号等によって、受信パケットを転送するか否かを判断するだけでは防止できない不正アクセスに関わるパケットを通過させないパケット転送機構、パケットを転送するか否かの判断を行なうための設定を利用者が行

ることを防ぐことのできるパケット転送機構、不正アクセスが為されていることを表示可能なパケット転送機構、等を容易に実現することのできるパケット転送装置、パケット転送方法、及びそのプログラムが格納された記憶媒体を提供することを目的とする。

【0028】

【課題を解決するための手段】上記目的を達成するために本発明のパケット転送装置は、複数のネットワークセグメントの間に設けられ、ネットワークセグメント相互間で転送されるパケットを監視するパケット転送装置であって、第1のネットワークセグメントを介して受信した受信パケットを第2のネットワークセグメントに送出する際に、予め設定された条件をもとに、前記受信パケットの情報に、前記第2のネットワークセグメントに接続された装置のソフトウェアに対し誤動作させる要因を含んでいるか否かを解析するパケット解析手段と、前記解析手段によって前記誤動作させる要因を含んだ情報をもつ不正パケットであることを判定した際に、当該不正パケットを破棄し、正常なパケットと判定した受信パケットのみを前記第2のネットワークセグメントに送出する手段とを具備してなることを特徴とする。

【0029】また本発明の装置は、少なくとも第1及び第2のネットワークセグメントに接続され、前記第1及び第2のネットワークセグメント相互の間で転送されるパケットに不正アクセスを起こすパケットが含まれる場合、その不正パケットを排除するパケット転送装置に於いて、前記第1のネットワークセグメントからのパケットを受信する受信手段と、前記受信手段で受信した受信パケットに識別子を付加する識別子付加手段と、前記識別子が付加された前記受信パケットを一時保留するパケット保留キューと、前記受信パケットが予め設定した既知の誤動作条件を含む不正アクセスのパケットであるか否かを判定し、不正アクセスに関わるパケットで無いことを判定した際に、当該受信パケットの識別子を出力するパケット解析手段と、前記パケット解析手段より出力された前記識別子を受信し、前記パケット保留キューから受信した前記識別子を持つ受信パケットを取り出し、前記第2のネットワークセグメントへ送出する送出手段とを具備することを特徴とする。

【0030】また本発明の装置は、少なくとも3つ以上のネットワークセグメントに接続され、複数の前記ネットワークセグメント間で転送されるパケットに不正アクセスを起こすパケットが含まれる場合、その不正パケットを排除するパケット転送装置に於いて、前記ネットワークセグメントからのパケットを受信する受信手段と、前記受信手段で受信した受信パケットに識別子を付加する識別子付加手段と、前記識別子が付加された前記受信パケットを一時保留するパケット保留キューと、前記受

スに関わるパケットで無いことを判定した際に、当該受信パケットの識別子を出力するパケット解析手段と、前記パケット解析手段より出力された前記識別子を受信し、前記パケット保留キューから受信した前記識別子を持つ受信パケットを取り出し、当該受信パケットに含まれる宛先MACアドレスから、送出すべきネットワークセグメントを判定する送出セグメント判定手段と、前記送出セグメント判定手段によって判定されたネットワークセグメントへ当該受信パケットを送出する1つ又は複数の送出手段とを具備することを特徴とする。

【0031】また本発明の装置は、少なくとも3つ以上のネットワークセグメントに接続され、複数の前記ネットワークセグメント間で転送されるパケットに不正アクセスを起こすパケットが含まれる場合、その不正パケットを排除するパケット転送装置に於いて、前記ネットワークセグメントからのパケットを受信する受信手段と、前記受信手段で受信した受信パケットに識別子を付加する識別子付加手段と、前記識別子が付加された前記受信パケットを送出先のネットワークセグメント毎に一時保留する複数のパケット保留キューと、前記識別子が付加された前記受信パケットに含まれる宛先MACアドレスから前記受信パケットの送出先ネットワークセグメントを判定し、当該ネットワークセグメントに対応する前記パケット保留キューに前記識別子が付加されたパケットを送出する送出セグメント判定手段と、前記受信パケットが予め設定した既知の誤動作条件を含む不正アクセスのパケットであるか否かを判定し、不正アクセスに関わるパケットで無いことを判定した際に、当該受信パケットの前記識別子を出力するパケット解析手段と、前記パケット保留キューに対応して設けられる複数の送出手段であって、前記パケット解析手段より出力された前記識別子を受信し、前記識別子を持つ受信パケットを保留している1つ又は複数の前記パケット保留キューから当該受信パケットを取り出し、対応付けられた前記ネットワークセグメントへ送出する送出手段とを具備することを特徴とする。

【0032】また本発明の装置は、過去に受信した不正アクセスに関わるパケットに含まれる文字列を記憶したデータベースを具備することを特徴とする。

【0033】また本発明の装置は、前記パケット解析手段により不正アクセスに関わるパケットであると判定された場合、その不正パケットの存在、構造、形式、受信時刻、送信元の少なくともいずれかを含む詳細情報を取得して保持する不正アクセス履歴保持手段と、前記不正アクセス履歴保持手段が保持する不正アクセス履歴を表示する不正アクセス履歴表示手段とを具備することを特徴とする。

【0034】また本発明の装置は、前記パケット解析手段により不正パケットであると判定された送出済パ

記パケット解析手段は不正パケットの解析時に、前記送出済パケット保持手段に保持された前記送出済パケットを参照することを特徴とする。

【0035】また本発明の装置は、前記受信パケットのヘッダ部のオプション、若しくはパラメータの組み合わせが、予め設定された既知の条件を満たしているか否かを判定する手段、前記受信パケットが搬送しているデータの長さ、若しくはデータが指定するパラメータの組み合わせが、予め設定された既知の条件を満たしているか否かを判定する手段、パケット相互のデータ構造、若しくはデータ内容が、予め設定された既知の条件を満たしているか否かを判定する手段、の少なくとも一つの手段により、不正アクセスに関わるパケットであるか否かを判定することを特徴とする。

【0036】また本発明の装置は、前記識別子が付加された受信パケットを格納するパケット格納手段と、不正アクセスのパケットに含まれる文字列を一部に内蔵するパケット解析プログラムが格納されるプログラム格納手段と、前記パケット解析プログラムに基づき、前記パケット格納手段に格納された受信パケットについて、既知の誤動作条件を含む不正アクセスのパケットであるか否かを判定し、不正アクセスに関わるパケットで無いことを判定した際に、当該受信パケットの識別子を出力するプログラム実行手段とを具備することを特徴とする。

【0037】また本発明の装置は、前記プログラム格納手段に格納された前記パケット解析プログラムを更新する解析プログラム更新手段を具備することを特徴とする。

【0038】また本発明の装置は、前記パケット転送装置に於いて、シリアルインタフェース、若しくはネットワークインタフェースでなる通信インタフェースと、前記通信インタフェースを介して受信したデータから、解析プログラム更新指示を示す特定の形式を満たしていることを識別する解析プログラム更新指示形式の識別手段とを具備し、前記解析プログラム更新指示形式の識別手段が前記解析プログラム更新指示であると識別したデータをもとに、前記パケット解析プログラムをロード、若しくは更新することを特徴とする。

【0039】また本発明の装置は、前記受信手段で受信したパケットから、前記パケット解析プログラムの更新指示を示す特定の形式を満たしているデータであることを識別する解析プログラム更新指示形式の識別手段を具備し、前記解析プログラム更新指示形式の識別手段が前記解析プログラム更新指示であると識別した受信パケットのデータをもとに、前記パケット解析プログラムをロードし、若しくは更新することを特徴とする。

【0040】また本発明の装置は、前記パケット内のデータ、若しくは前記シリアルインタフェースを介して入

出し、当該電子署名情報が正当な署名であるか否かを判定し、正当であると判定した場合、前記パケット解析プログラムをロードし、若しくは更新することを特徴とする。

【0041】また本発明の装置は、前記パケット解析手段が不正アクセスに関わるパケットであると判定した場合、その不正パケットの存在、構造、形式、受信時刻、送信元等の少なくともいずれかを含む詳細情報を他の装置に通知する装置内情報通知手段を具備することを特徴とする。

【0042】また本発明の装置は、前記パケット解析プログラムの設定または更新に伴う通信、若しくは不正パケットの前記詳細情報を他の装置に通知する通信である特定通信のみに使用する送信元アドレスを予め設定する通信用アドレス設定手段と、前記通信用アドレス設定手段により設定された通信用アドレスを保持する通信用アドレス保持手段と、前記特定通信を行わないときは、前記送信元アドレス宛てに送られるパケットを破棄し、前記特定通信を行うときのみ、前記送信元アドレス宛てのパケットを受信する通信制御手段とを具備してなることを特徴とする。

【0043】また本発明の装置は、前記パケット解析プログラムの設定または更新に伴う通信、若しくは不正パケットの前記詳細情報を他の装置に通知する通信である特定通信のみに使用する送信元アドレスとして、当該特定通信の送出先ネットワークセグメントとは異なるネットワークセグメントから過去に受信したパケットの送信元アドレスの1つを選択する通信用アドレス選択手段と、前記通信用アドレス選択手段で選択された送信元アドレスを宛先としたパケットのうち、当該特定通信に関

わるパケットを横奪するパケット横奪手段とを具備することを特徴とする。

【0044】また本発明の装置は、転送対象であるパケットから前記特定通信の開始指示である特定の形式を満たしているデータであることを識別して、前記特定通信を開始する通信開始指示形式識別手段を具備することを特徴とする。

【0045】また本発明の装置は、前記通信開始指示形式識別手段は、データ中に含まれている電子署名が正当な署名であるか否かを判定し、正当な署名であると判定した場合のみ当該データを通信開始指示であると識別する電子署名識別手段を具備することを特徴とする。

【0046】上記目的を達成するために、本発明のパケット転送方法は、複数のネットワークセグメントの間に設けられ、ネットワークセグメント相互間で転送されるパケットを監視するパケット転送装置であって、第1のネットワークセグメントより受信した受信パケットを第2のネットワークセグメントに送出する際に、予め設定された条件に基づいて、前記受信パケットの種類に、前記

トウェアに対し誤動作させる要因を含んでいるか否かを判定し、前記誤動作させる要因を含んだ情報をもつ不正パケットであることを判定した際に、当該不正パケットを破棄し、正常なパケットと判定した受信パケットを前記第2のネットワークセグメントに送出することを特徴とする。

【0047】また本発明の方法は、少なくとも第1及び第2のネットワークセグメントに接続され、前記第1及び第2のネットワークセグメント相互の間で転送されるパケットに不正アクセスを起こすパケットが含まれる場合、その不正パケットを排除するパケット転送方法に於いて、前記第1のネットワークセグメントからのパケットを受信するステップと、前記受信した受信パケットに識別子を付加するステップと、前記識別子が付加された前記受信パケットを一時保留するステップと、前記識別子が付加された前記受信パケットを解析し、不正アクセスに関わるパケットでないことを判定し、判定した正常な受信パケットの前記識別子を出力するステップと、前記識別子を受信し、前記一時保留されている前記受信パケットの中から、受信した前記識別子を持つ前記受信パケットを取り出し、前記第2のネットワークセグメントに送出するステップとを具備することを特徴とする。

【0048】また本発明の方法は、少なくとも3つ以上のネットワークセグメントに接続され、複数の前記ネットワークセグメント間で転送されるパケットに不正アクセスを起こすパケットが含まれる場合、その不正パケットを排除するパケット転送方法に於いて、前記ネットワークセグメントの一つからパケットを受信するステップと、前記受信した受信パケットに識別子を付加するステップと、前記識別子が付加された前記受信パケットを一時保留するステップと、前記識別子が付加された前記受信パケットを解析し、不正アクセスに関わるパケットでないことを判定し、判定した正常な受信パケットの前記識別子を出力するステップと、前記識別子を受信し、前記一時保留されている前記受信パケットの中から、受信した前記識別子を持つ前記受信パケットを取り出し、当該受信パケットに含まれるMACアドレスから送出すべきネットワークセグメントを判定するステップと、前記判定されたネットワークセグメントに対し、取り出した前記受信パケットを送出するステップとを具備することを特徴とする。

【0049】また本発明の方法は、少なくとも3つ以上のネットワークセグメントに接続され、複数の前記ネットワークセグメント間で転送されるパケットに不正アクセスを起こすパケットが含まれる場合、その不正パケットを排除するパケット転送方法に於いて、前記ネットワークセグメントの一つからパケットを受信するステップと、前記受信した受信パケットに識別子を付加するステップと、前記識別子が付加された前記受信パケットを一時保留するステップと、前記識別子が付加された前記受信パケットを解析し、不正アクセスに関わるパケットでないことを判定し、判定した正常な受信パケットの前記識別子を出力するステップと、前記識別子を受信し、前記一時保留されている前記受信パケットの中から、受信した前記識別子を持つ前記受信パケットを取り出し、当該受信パケットに含まれるMACアドレスから送出すべきネットワークセグメントを判定するステップと、前記判定されたネットワークセグメントに対し、取り出した前記受信パケットを送出するステップとを具備することを特徴とする。

先ネットワークセグメントを判定し、前記送出先のネットワークセグメント毎に設けられた一時保留キューに、前記判定に従って前記受信パケットを格納するステップと、前記識別子が付加された前記受信パケットを解析し、不正アクセスに関わるパケットでないことを判定し、判定した正常な受信パケットの前記識別子を出力するステップと、前記識別子を受信し、前記一時保留キューの前記受信パケットの中から、受信した前記識別子を持つ前記受信パケットを取り出し、対応するネットワークセグメントに送出するステップとを具備することを特徴とする。

【0050】上記目的を達成するために、本発明のコンピュータ読み取り可能な記憶媒体は、少なくとも2つ以上のネットワークセグメント相互の間で転送されるパケットを監視するパケット転送装置に記憶され、前記ネットワークセグメントの一方からのパケットを受信する機能と、前記受信した受信パケットに識別子を付加する機能と、前記識別子が付加された前記受信パケットを一時保留する機能と、前記識別子が付加された前記受信パケットを解析し、不正アクセスに関わるパケットでないことを判定した際に、当該受信パケットの識別子を出力する機能と、前記識別子を受信し、前記一時保留されているパケットの中から受信した前記識別子を持つ受信パケットを取り出し、送出先の他方のネットワークセグメントへ送出する機能とを実現するためのプログラムが記憶される。

【0051】また本発明の記憶媒体は、少なくとも3つ以上のネットワークセグメント間で転送されるパケットを監視するパケット転送装置に記憶され、前記ネットワークセグメントの一つからパケットを受信する機能と、前記受信した受信パケットに識別子を付加する機能と、前記識別子が付加された前記受信パケットを一時保留する機能と、前記識別子が付加された前記受信パケットを解析し、不正アクセスに関わるパケットでないことを判定した際に、当該受信パケットの識別子を出力する機能と、前記識別子を受信し、前記一時保留されている受信パケットの中から受信した前記識別子を持つ受信パケットを取り出し、当該受信パケットに含まれるMACアドレスから送出すべきネットワークセグメントを判定する機能と、前記判定されたネットワークセグメントへ当該受信パケットを送出する機能とを実現するためのプログラムが記憶される。

【0052】また本発明の記憶媒体は、少なくとも3つ以上のネットワークセグメント間で転送されるパケットを監視するパケット転送装置に記憶され、前記ネットワークセグメントの一つからパケットを受信する機能と、前記受信した受信パケットに識別子を付加する機能と、前記識別子が付加された前記受信パケットに含まれるMACアドレスから、送出すべきネットワークセグメント

ケットを、前記判定された送出先ネットワークセグメント毎に分けて一時保留する機能と、前記識別子が付加された前記受信パケットを解析し、不正アクセスに関わるパケットでないことを判定した際に、当該受信パケットの識別子を出力する機能と、前記識別子を受信し、前記一時保留されている前記受信パケットの中から、受信した前記識別子を持つ受信パケットを取り出し、当該受信パケットを、前記判定された送出先ネットワークセグメントへ送出する機能とを実現するためのプログラムが記憶される。

【0053】上記したような不正アクセスに関わるパケットを排除する機能をもつことにより、複数のネットワークセグメントに接続され、セグメント相互の間でパケットを転送するパケット転送装置に於いて、宛先/送信元MACアドレスや、さらに上位のプロトコルの宛先/送信元アドレスやサービス番号等によってパケットを転送するか否かを判断するだけでは防止できない、不正アクセスに関わるパケットを通過させないパケット転送装置を実現することができる。

【0054】また、パケットを転送するか否かの判断を行なうための設定を利用者が行なうことなく、不正アクセスに関わるパケットを通過させないパケット転送装置を実現することができる。

【0055】また、IPアドレス等のネットワークアドレスを全く持たないため、自身が不正アクセスの対象となることを防げる、不正アクセスに関わるパケットを通過させないパケット転送装置を実現することができる。

【0056】また、不正アクセスが為されていることを表示可能なパケット転送装置を実現することができる。

【0057】

【発明の実施の形態】以下、図面を参照して本発明の実施形態を説明する。

【0058】先ず図1を参照して本発明の第1実施形態を説明する。

【0059】図1は本発明の第1実施形態によるパケット転送装置の要部の構成要素を示すブロック図である。この図1に示す第1実施形態では、パケット転送装置の片方向の転送についてのみ、不正アクセスに関わるパケットの通過を防ぐ機能を備えた構成を例示している。

【0060】図1に示すパケット転送装置10に於いて、パケット受信部11と、パケット送出部14は、それぞれ異なるネットワークセグメント（セグメントA—セグメントB）相互の間に接続される。ここではパケット受信部11が接続されているネットワークセグメントAから、パケット送出部14が接続されているネットワークセグメントBへパケットを転送する例を示している。

【0061】パケット受信部11は、ネットワークセグメントA上のパケットを受信する。パケット識別子が付加

10

20

30

40

ケット保留キュー13は識別子を付加されたケットを、パケット解析機構15が、不正アクセスに関わるパケットで無いことを判定するまで一時保留する。パケット解析機構15は、受信パケットを送出し、不正アクセスに関わるパケットで無いことを判定したパケットの識別子をパケット送出部14に伝える。パケット送出部14は、パケット解析機構15から伝えられた識別子と同じ識別子が付加されている受信パケットをパケット保留キュー13から取り出し、当該パケットをネットワークセグメントBへ送出する。

【0062】ここで、上記各図を参照して本発明の第1実施形態に於ける動作を説明する。

【0063】図1に示すパケット転送装置10に於いて、パケット受信部11はネットワークセグメントAに接続される送信側システム（又は端末、又は装置）から送信されたパケットを順次受信する。

【0064】パケット識別子付加機構12は、受信されたパケットに、装置内でユニークな識別子を付加する。この際の識別子としては、例えば、1、2、3、4と連番を付してゆく方法がある。また、パケットの到着時刻を用いる方法もある。あるいは、パケットを格納した記憶装置の番地を利用する方法もある。

【0065】上記パケット識別子付加機構12により識別子が付加されたパケットは、パケット保留キュー13に格納されるとともに、パケット解析機構15に渡される。

【0066】パケット解析機構15には、予め、不正アクセスに関わるパケットを識別するための判定情報が格納されているデータベース150が設けられる。このデータベース150には、少なくとも過去に受信した不正アクセスに関わるパケットに含まれていた文字列（判定情報）が格納されている。

【0067】パケット識別子付加機構12から受信パケットを渡されたパケット解析機構15は、当該受信パケットをデータベース150に格納された判定情報に基づいて、不正アクセスに関わるか否かを判定する。データベース150には判定情報として、不正アクセスに関わるパケットに含まれる文字列の一覧が格納されている。パケット解析機構15は、データベース150に格納された文字列一覧に含まれる文字列を受信パケットと逐次比較し、当該文字列一覧に含まれる文字列のいずれかが、受信パケットに含まれていた場合、当該受信パケットが不正アクセスに関わるものであると判定できる。受信パケットが不正アクセスに関わるものでは無いパケットであると判定した場合、パケット解析機構15は、当該受信パケットに付加された識別子をパケット送出部14に伝える。

【0068】識別子を伝えられたパケット送出部14は、パケット保留キュー13から、当該識別子に基づいて

して受信側システム（又は端末、又は装置）に送出する。

【0069】パケット解析機構15に於いて、不正アクセスに関わるパケットであると判定された受信パケットは、パケット保留キュー13に残され、明示的な指示あるいは、パケット保留キュー13からの溢れによる等の暗黙的な手段によって破棄される。

【0070】この一連の動作によって、不正アクセスに関わるパケットを通過させないパケット転送装置を実現することができる。

【0071】また、パケット解析機構15のデータベース150に格納される、不正アクセスに関わるパケットを識別するための判定情報には、パケットデータの内容に関わるものをも含めることが可能であるため、宛先/送信元MACアドレスや、さらに上位のプロトコルの宛先/送信元アドレスやサービス番号等によって、パケットを転送するか否かを判断するだけでは防止できない不正アクセスに関わるパケットを通過させないパケット転送装置を実現することができる。

【0072】また、このパケット解析機構15のデータベース150に予め格納される、不正アクセスに関わるパケットを識別するための判定情報は、利用者や設置場所によらず、同一のものを利用可能であるため、利用者がパケットを転送するか否かの判断を行なうための設定を行なうことなく不正アクセスに関わるパケットを通過させないパケット転送装置を実現することができる。

【0073】また、このパケット転送装置自身は、その動作を行なう上で、IPアドレス等のネットワークアドレスを全く持つ必要が無いため、自身が不正アクセスの対象となることを防ぎ、不正アクセスに関わるパケットを通過させないパケット転送装置を実現することができる。さらに、パケットデータの内容も、不正アクセスに関わるパケットを識別するための情報として利用することが可能であるため、明らかに不正アクセスに関わるパケットであるものを判定可能となる。例えば、アプリケーションプログラムに対して、規定より異常に長い文字列を送るようなパケットは、明らかに不正アクセスに関わるパケットであると判定できる。また、特定のデータ列が、アプリケーションプログラムやOSの誤動作を引き起こすことが知られている場合、当該データ列を含むパケットは、やはり、明らかに不正アクセスに関わるパケットであると判定できる。これらの、明らかに不正アクセスに関わるパケットであると判定できるパケットであると送出した場合に、利用者に表示することで、不正アクセスが成されていること、あるいは成されたことを表示可能なパケット転送装置を実現することができる。

【0074】次に図2を参照して本発明の第2実施形態を説明する。

【0075】図2は本発明の第2実施形態によるパケッ

【0076】この図2に示す第2実施形態では、パケット転送装置の両方向の転送について、不正アクセスに関わるパケットの通過を防ぐ機能を備えた構成を例示している。

【0077】この図2に示すパケット転送装置20は、ネットワークセグメントAからネットワークセグメントBへの不正アクセスに関わるパケットの通過を防ぐことができるとともに、ネットワークセグメントBからネットワークセグメントAへの不正アクセスに関わるパケットの通過を防ぐことができる。

【0078】即ち、パケット転送装置20に於いて、パケット受信部21aはネットワークセグメントAより一つのパケットを受信する。

【0079】パケット識別子付加機構22aは、受信されたパケットに、装置内でユニークな識別子を付加する。

【0080】上記パケット識別子付加機構22aにより識別子が付加された受信パケットは、パケット保留キュー23aに格納されるとともに、パケット解析機構25aに渡される。パケット解析機構25aのデータベース250aには、予め不正アクセスに関わるパケットを識別するための判定情報が格納されている。

【0081】パケット識別子付加機構22aからパケットを渡されたパケット解析機構25aは、受信パケットをデータベース250aに格納された判定情報に基づいて解析し、受信パケットが不正アクセスに関わるか否かを判定する。受信パケットが不正アクセスに関わるものではないパケットであると判定した場合、パケット解析機構25aは、当該受信パケットに付加された識別子をパケット送出部24bに伝える。この識別子を受信したパケット送出部24bは、パケット保留キュー23aから、当該識別子を持つ受信パケットを取り出し、ネットワークセグメントBに送出する。

【0082】パケット解析機構25aに於いて、不正アクセスに関わるパケットであると判定された受信パケットは、パケット保留キュー23aに残され、明示的な指示あるいは、パケット保留キュー23aからの溢れによる等の暗黙的な手段によって破棄される。

【0083】一方、パケット受信部21bはネットワークセグメントBより一つのパケットを受信する。パケット識別子付加機構22bは、受信したパケットに、装置内でユニークな識別子を付加する。

【0084】上記パケット識別子付加機構22bにより識別子が付加された受信パケットは、パケット保留キュー23bに格納されるとともに、パケット解析機構25bに渡される。パケット解析機構25bのデータベース250bには、予め不正アクセスに関わるパケットを識別するための判定情報が格納されている。

【0085】パケット識別子付加機構22bから受信パ

ットをデータベース250bに格納された判定情報に基づいて解析し、受信パケットが不正アクセスに関わるか否かを判定する。受信パケットが不正アクセスに関わるものではないパケットであると判定した場合、パケット解析機構25bは、当該受信パケットに付加された識別子をパケット送出部24aに伝える。

【0086】識別子を伝えられたパケット送出部24aは、パケット保留キュー23bから、当該識別子を持つ受信パケットを取り出し、ネットワークセグメントAに送出する。

【0087】パケット解析機構25bに於いて、不正アクセスに関わるパケットであると判定された受信パケットは、パケット保留キュー23bに残され、明示的な指示あるいは、パケット保留キュー23bからの溢れによる等の暗黙的な手段によって破棄される。

【0088】このような動作によって、ネットワークセグメントAからネットワークセグメントBへのパケット転送、およびネットワークセグメントBからネットワークセグメントAへのパケット転送について、その何れに於いても不正アクセスに関わるパケットを通過させないパケット転送装置を実現することができる。

【0089】次に図3を参照して本発明の第3実施形態を説明する。

【0090】図3は本発明の第3実施形態によるパケット転送装置の要部の構成要素を示すブロック図である。

【0091】この図3に示す第3実施形態では、パケット転送装置の片方向の転送について、不正アクセスに関わるパケットの通過を防ぐ機能を備えた構成を例示している。

【0092】この図3に示すパケット転送装置30は、上記図2に示す第2実施形態の構成の簡素化を図ったもので、ネットワークセグメントAからネットワークセグメントBへの不正アクセスに関わるパケットに関してはその通過を防ぐが、ネットワークセグメントBからネットワークセグメントAへのパケット転送についてはパケットの通過を防げない構成としている。この図3に示す構成のパケット転送装置30は、外部ネットワークとの接続点に設けられるような場合（例えばネットワークセグメントBに接続されるシステムにおいて自己管理が可能な構内等のネットワークシステムであり、ネットワークセグメントAが外界のネットワークシステムであるような場合）に、上記図2に示す第2実施形態に示すパケット転送装置20に比して構成を簡素化できる。

【0093】パケット転送装置30に於いて、パケット受信部31aはネットワークセグメントAより一つのパケットを受信する。パケット識別子付加機構32は、パケット受信部31aからの受信パケットに対し、装置内でユニークな識別子を付加する。

【0094】上記パケット識別子付加機構32により

33に格納されるとともに、パケット解析機構35に渡される。パケット解析機構35のデータベース350には、予め不正アクセスに関わるパケットを識別するための判定情報が格納されている。

【0095】パケット識別子付加機構32から受信パケットを渡されたパケット解析機構35は、受信パケットをデータベース350に格納された識別情報に基づいて解析し、受信パケットが不正アクセスに関わるか否かを判定する。受信パケットが不正アクセスに関わるものでは無いパケットであると判定した場合、パケット解析機構35は、当該受信パケットに付加された識別子をパケット送出部34bに伝える。

【0096】識別子を伝えられたパケット送出部34bは、パケット保留キュー33から、当該識別子を持つ受信パケットを取り出し、ネットワークセグメントBに送出する。

【0097】パケット解析機構35に於いて、不正アクセスに関わるパケットであると判定されたパケットは、パケット保留キュー33に残され、明示的な指示あるいは、パケット保留キュー33からの溢れによる等の暗黙的な手段によって破棄される。

【0098】一方、パケット受信部31bはネットワークセグメントBより一つのパケットを受信すると、当該パケットをそのまま（スルーモードで）パケット送出部34aに渡す。パケット送出部34aは、パケット受信部31bより受けたパケットをネットワークセグメントAに送出する。

【0099】このような動作によって、ネットワークセグメントAからネットワークセグメントBへのパケット転送については、不正アクセスに関わるパケットを通過させることないよう厳重に管理され、逆方向の転送については不正アクセスに関する防御機能を簡略したパケット転送装置を実現することができる。

【0100】次に図4、図5を参照して本発明の第4実施形態、および第5実施形態を説明する。

【0101】図4は、本発明の第4実施形態によるパケット転送装置の要部の構成要素を示すブロック図であり、図5は、本発明の第5実施形態によるパケット転送装置の要部の構成要素を示すブロック図である。

【0102】この図4および図5に示す各実施形態では、何れに於いても、送出すべきネットワークセグメントを判定できた場合、判定されたネットワークセグメントのみに送出することで、判定されたネットワークセグメント以外のネットワークセグメントのトラフィックを削減することを可能にしている。

【0103】本発明に係るパケット転送装置が、3つ以上のネットワークセグメント間でパケットを転送する場合、あるネットワークセグメントから受信したパケットを、当該ネットワークセグメント以外の全てのネットワ

の宛先MACアドレスから、送出すべきネットワークセグメントを判定し、判定できた場合は、判定されたネットワークセグメントのみに送出することで、判定されたネットワークセグメント以外のネットワークセグメントのトラフィックを削減する方法もある。

【0104】図4に示す第4実施形態では、各送出セグメントに対して、パケット保留キューを共通としたパケット転送装置40の構成を示している。ここでは、パケット解析機構45により、パケットが不正アクセスに関わるか否かを判定した後に、送出すべきネットワークセグメントを判定する構成としている。

【0105】上記図4に示す構成のパケット転送装置40に於いて、パケット受信部41により受信され、パケット識別子付加機構42によって識別子が付加された受信パケットは、全ての送出セグメントに共通のパケット保留キュー43に格納される。

【0106】パケット解析機構45はデータベース450に格納された判定情報に基づき、受信パケットが不正アクセスに関わるか否かを判定し、不正アクセスに関わるパケットでは無いと判定した場合、当該受信パケットの識別子を送出セグメント判定機構46に通知する。

【0107】パケット解析機構45より識別子を通知された送出セグメント判定機構46は、当該識別子を持つ受信パケットをパケット保留キュー43から取り出し、受信パケットの宛先MACアドレスから、送出すべきネットワークセグメントを識別し、識別できた場合は、判定されたネットワークセグメントに対応する少なくとも一つのパケット送出部（44a～44nのいずれか）に受信パケットを受け渡す。そして、パケット送出部は識別したネットワークセグメントに受信パケットを送出する。また、ネットワークセグメントが識別できなかった場合は、全てのパケット送出部44a～44nに受信パケットが送られ、パケット送出部44a～44nに接続されるネットワークセグメントに受信パケットが送出される。

【0108】図5に示す第5実施形態では、送出ネットワークセグメントそれぞれに固有のパケット保留キューを設けたパケット転送装置50の構成を示している。ここでは、パケット解析機構55により受信パケットが不正アクセスに関わるか否かを判定する以前に、送出すべきネットワークセグメントを判定する構成としている。

【0109】図5において、パケット受信部51に受信され、パケット識別子付加機構52によって識別子が付加された受信パケットは、送出セグメント判定機構56およびパケット解析機構55に渡される。

【0110】送出セグメント判定機構56は、パケット受信部51で受信され、パケット識別子付加機構52によって識別子が付加された受信パケットの宛先MACアドレスから、送出すべきネットワークセグメントを識別

ケット保留キュー（53a～53nのいずれか）に当該受信パケットを格納する。

【0111】パケット保留キュー53a～53nは、送出セグメント判定機構56によって格納された受信パケットを、パケット解析機構55によって不正アクセスに関わるパケットで無いことが判定されるまで一時保留する。そして、このパケット保留キュー53a～53nに対応してパケット送出部54a～54nがそれぞれ接続されている。

【0112】パケット解析機構55は、データベース550に格納された判定情報に基づき、受信パケットが不正アクセスに関わるか否かを判定し、受信パケットが不正アクセスに関わるパケットでは無いと判定した場合、当該受信パケットの識別子をパケット送出部54a～54nに通知する。

【0113】パケット解析機構55より識別子を通知されたパケット送出部54a～54nは、当該識別子を持つ受信パケットが対応して接続されているパケット保留キュー53a～53nに存在するとき、当該受信パケットを取り出し、対応するネットワークセグメントに送出する。

【0114】また、送出セグメント判定機構56は、送出すべきネットワークセグメントが認識できなかった場合は、受信パケットを全てのパケット保留キュー53a～53nに格納する。そして、受信パケットがパケット解析機構55より不正アクセスではないと判定され、当該受信パケットの識別子がパケット送出部54a～54nに通知された時、パケット送出部54a～54nはパケット保留キュー53a～53nから受信パケットを取り出し、対応する全てのネットワークセグメントにそのパケットを送出する。

【0115】このような構成とすることにより、パケット解析機構55で不正アクセスに関わるパケットでは無いと判定されてからパケット送出部（54a～54n）へ送出されるまでの時間が短縮できる効果がある。

【0116】そして、上記した第4実施形態、第5実施形態によれば、送出すべきネットワークセグメントを識別できた場合は、識別されたネットワークセグメントのみにパケットの送出を行なうことで、識別されたネットワークセグメント以外のネットワークセグメントのトラフィックを削減することが可能となる。

【0117】次に、図6乃至図8を参照して本発明の第6実施形態を説明する。

【0118】図6は、本発明の第6実施形態によるパケット転送装置の要部の構成要素を示すブロック図である。図7および図8は、それぞれ第6実施形態に於ける不正アクセス表示手段の例を示す図である。

【0119】この図6に示す第6実施形態のパケット転送装置60は、パケット解析機構65が不正アクセスに関

在、構造、形式、受信時刻、送信元の少なくともいずれかを含む詳細情報を不正アクセス履歴として記録し表示する機能を備えている。

【0120】不正アクセス履歴保持機構66は、パケット解析機構65が不正アクセスに関わるパケットであるという判定した受信パケットについて、その存在、および受信時刻、送信元等の詳細情報をパケット解析機構65より取得し、保持する。

【0121】不正アクセス履歴表示機構67は、不正アクセス履歴保持機構66が保持する不正アクセス履歴を表示するものである。この際不正アクセス履歴表示機構67の具体例を図7、図8にそれぞれ示している。

【0122】上記図6に示す構成のパケット転送装置60に於いて、パケット識別子付加機構62は、パケット受信部61で受信された受信パケットに、装置内でユニークな識別子を付加する。

【0123】上記パケット識別子付加機構62により識別子が付加された受信パケットは、パケット保留キュー63に格納されるとともに、パケット解析機構65に渡される。

【0124】パケット識別子付加機構62から受信パケットを渡されたパケット解析機構65は、データベース650に格納された判定情報に基づき解析し、当該受信パケットが不正アクセスに関わるか否かを判定する。

【0125】したがって、パケット解析機構65はパケット受信部61を介して不正アクセスに関わるパケットが受信されると、当該受信パケットが不正アクセスであると判定する。この際、パケット解析機構65は、当該受信パケットの識別子をパケット送出部64へ送出せず、不正アクセスに関わるパケットが受信側ネットワークセグメントに転送されないことは上記した各実施形態と同様である。

【0126】この第6実施形態に於いては、上記パケット解析機構65が不正アクセスに関わるパケットであると判定した際、不正アクセス履歴保持機構66に不正アクセスの存在、並びに受信時刻や送信元、送信先、不正の種類などの情報を不正アクセス履歴情報として送出する。

【0127】不正アクセス履歴保持機構66は、上記パケット解析機構65より取得した不正アクセス履歴を保持し、利用者が不正アクセス履歴の消去の作業を行なうまでそれを保持する。

【0128】不正アクセス履歴表示機構67は、不正アクセス履歴保持機構66に保持されている、不正アクセスに関わるパケットの存在、受信時刻、送信元、送信先、およびパケット解析機構65が判定した不正の種類等の不正アクセス履歴情報の内容を表示する。

【0129】この際不正アクセス履歴表示機構67の具体的な構成例として、図7に示すように、パケ...

用いた不正アクセス表示器67Aを点灯駆動して、不正アクセスの存在を利用者に報知する構成とする。または、図8に示すように、不正アクセスの時刻、送信元、送信先、不正の種類などを例えばLCD等を用いた不正アクセス表示装置67Bに文字表示して、利用者に、不正アクセスの時刻、送信元、送信先、不正の種類などの詳細情報を報知する構成とする。さらに、履歴情報を遡って表示するためのスイッチを備えて、利用者が、不正アクセスの履歴情報を遡って確認できるようにすることもできる。

【0130】次に、図9乃至図12を参照して本発明の第7実施形態を説明する。

【0131】図9は、本発明の第7実施形態によるパケット転送装置の要部の構成要素を示すブロック図である。

【0132】この図9に示す第7実施形態のパケット転送装置70は、複数のパケットが必要なパケットの解析時に参照される送出済みのパケットを保持する送出済みパケット保持機構76を具備したことを特徴とする。

【0133】送出済みパケット保持機構76は、パケット解析機構75が受信パケットを送出する際に参照されるもので、パケット解析機構75が解析処理した送出済みのパケットを保持する機能をもつ。

【0134】パケット解析機構75は、パケット受信部71がパケットを受信し、パケット識別子付加機構72が識別子を付加した受信パケットを解析する際に、当該受信パケットに加えて、当該受信パケット以前に送出した送出済みパケットをあわせて参照し、不正アクセスに関わるパケットであるか否かを判定する。

【0135】上記図9に示す構成のパケット転送装置70に於いて、パケット受信部71で受信され、パケット識別子付加機構72により識別子が付加された受信パケットは、パケット保留キュー73に格納され、パケット解析機構75に渡されると同時に送出済みパケット保持機構76に保持される。

【0136】パケット解析機構75は、パケット識別子付加機構72から渡された受信パケットを送出する際に、装置内に組み込まれた後述するパケット解析プログラムによる判定情報（他の実施形態と同様にデータベースを参照しても良い）、および送出済みパケット保持機構76に保持されている当該受信パケット以前に送出したパケットを含めて参照（この参照では、過去に正常なパケットと判定したことを示す）し、パケット識別子付加機構72から渡された受信パケットが不正アクセスに関わるパケットであるか否かを判定する。

【0137】パケット解析機構75は、パケット解析プログラムの解析に基づいて、受信パケットが不正アクセスに関わるパケットであると判定した場合、送出済みパケット保持機構76に保持されている当該受信パケット

以降の解析において、送出したパケットのみを参照することとなり、より正確な解析を可能とする。

【0138】送出済みパケット保持機構76に、保持されているパケットを、例えば、格納してから一定期間過ぎたら破棄する方法や、宛先毎に予め指定した特定のデータ量を越えたら、越えた分、到着順序に従い破棄する方法などによって、送出済みパケット保持機構76に新しいパケットが格納できなくなることを防ぐ機構が設けられる。

【0139】また、送出済みパケット保持機構76に、パケット解析機構75からの送出済みパケットの参照が容易となるように、例えば、特定の宛先へのパケットのみを取り出す機能や、パケットに含まれる連番の順にパケットを並び替えて取り出す機能が設けられる。これにより、アプリケーションプログラムやOS等に対してバグを引き起こすことが知られている特定のデータ列が、複数のパケットに跨って送られてきた場合など、受信パケットをそれぞれ別個に判定しては見逃してしまうような不正アクセスに関わるパケットであっても見つけることが可能となる。

【0140】図10は、上述したパケット解析プログラムを用いたパケット解析機構の構成例を示すブロック図である。ここでは、図9に示す第7実施形態に於けるパケット解析機構75を例にとって示しているが、上述した第1乃至第6の実施形態に示した不正パケット解析用データベースの変わりに、パケット解析機構を適用しても良い。

【0141】図10に示すパケット転送装置のパケット解析機構75は、実行プログラムの形式で不正アクセスに関わるパケットの判定を行う処理機能が実現される。

【0142】図10に示すパケット解析機構75に於いて、パケット格納部751は、命令実行機構754からメモリ制御機構753を介してアクセスされる記憶装置であり、パケット識別子付加機構72により識別子が付加された受信パケットや、送出済みパケット保持機構76に保持されている送出済みパケットが格納される。

【0143】実行命令格納部752は、命令実行機構754が動作するのに必要なパケット解析プログラムを格納する記憶装置である。

【0144】メモリ制御機構753は、命令実行機構754からのアクセス要求に基づき、パケット格納部751、あるいは実行命令格納部752、あるいはその他の記憶装置と命令実行機構754との間で、格納されたデータを受け渡す機能を持つ。

【0145】命令実行機構754は、メモリ制御機構753から渡されるパケット解析プログラムに従い、パケット格納部751に格納されたパケットが、不正アクセスに関わるパケットであるか否かを判定するためのパケット解析処理を実行する。

り、受信パケットが不正アクセスに関わるパケットであるか否かが判定される。そして、当該受信パケットが不正アクセスに関わるパケットで無い場合は、当該受信パケットを送出すべく、パケット送出部74（あるいは図4、図5に示す送出セグメント判定機構46、56）に、当該受信パケットの識別子が伝えられる。

【0147】ここで、図10に示す構成のパケット解析機構75に於ける処理動作を、図9に示すパケット転送装置70を適用した場合を基に説明する。

【0148】図10に示す構成のパケット解析機構75に於いて、実行命令格納部752には、命令実行機構754が動作するのに必要なパケット解析プログラムが予め格納されている。

【0149】図9に示すパケット転送装置70に於いて、パケット受信部71で受信されたパケットはパケット識別子機構72によって識別子が付加される。この識別子が付加された受信パケットは、パケット保留キュー73に格納され、またパケット解析機構75に渡されると同時に、送出済みパケット保持機構76にも格納される。パケット解析機構75に渡されたパケットは、パケット格納部751に格納される。

【0150】パケット格納部751に受信パケットを格納する方法としては、パケット識別子付加機構72、または送出済みパケット保持機構76から受信パケットをコピーしてくる方法。または、パケット識別子付加機構72や送出済みパケット保持機構76と記憶装置（パケット格納部751）を共有する方法等がある。送出済みパケット保持機構76を持つ場合、送出済みパケット保持機構76に保持されている送出済みパケットもパケット格納部751に格納する構成にしてもよい。

【0151】パケット格納部751へのパケットの格納が完了すると、命令実行機構754の動作が開始される。命令実行機構754は、メモリ制御機構753を介して実行命令格納部752に格納されたパケット解析プログラム（実行プログラム）を先頭から逐次読み出して送出処理を実行する。

【0152】例えば、パケット格納部751に格納された受信パケットに、不正アクセスに関わるパケットに含まれる文字列が含まれているか否かを解析する場合、実行命令格納部752に格納されたパケット解析プログラムの一部には、不正アクセスに関わるパケットに含まれる文字列の一覧が含まれており、命令実行機構754は、メモリ制御機構753を介して、当該文字列一覧に含まれる文字列と受信パケットを逐次比較して、当該文字列一覧に含まれる文字列のいずれかが受信パケットに含まれていた場合、当該受信パケットが不正アクセスに関わるものであると判定する。

【0153】また、命令実行機構754は、実行命令格納部752に格納されたパケット解析プログラムに従

の宛先への受信パケットのみを取り出す機能や、受信パケットに含まれる連番順にパケットを並び替えて取り出す機能等を利用して、送出済みパケット保持機構76から送出済みのパケットを取り出し、パケット格納部751に格納する機能を持つこともできる。

【0154】命令実行機構754はパケット解析プログラムの終端まで処理を実行し、受信パケットが不正アクセスに関わるものであるか否かを判定する。

【0155】このような不正アクセスに関わるパケットの判定機能をもつ構造とすることで、例えば、OSの誤動作を引き起こすことが知られている特定のデータ列として、一部のみ異なる複数のデータ列がある場合、共通する部分の比較は一度で完了することが可能となり、不正アクセスに関わるものであるか否かの判定をより高速に行なうことが可能となる。さらに、命令実行機構754の動作が停止している期間に、実行命令格納部752の実行プログラムを入れ替えると、次のパケットを受信した際に、新しく入れ替えられた実行プログラムにしたがって、解析が開始されることから、パケット解析機構75の不正アクセスの解析手段を更新することも容易となる。

【0156】図11及び図12のフローチャートは、実行命令格納部752に格納されるパケット解析プログラムを命令実行機構754が実行して、不正アクセスに関わるパケットの判定処理の具体例な処理手順を示す。

【0157】この図11及び図12に示す判定処理では、上記パケット格納部751に格納された受信パケットについて、先ずヘッダフィールドのオプションや、パラメータの組み合わせがパケット転送先のサーバに誤動作を引き起こすとして予め設定された既知の条件を満たしているか否かが判定される（図11ステップS11）。即ち、受信パケットのヘッダ部から不審な相手からの送信であったり、形式の異なる怪しいパケットであることを見分ける処理を行なう。

【0158】ここで上記条件を満たしていれば、当該受信パケットは破棄の対象となる（図11ステップS15）。一方、上記条件を満たしていなければ、次に、断片化されたパケットやTPC等、判断に他のパケットの情報も必要となるか否かが判断される（図11ステップS12）。

【0159】他のパケットを必要としない場合は、次にパケットが搬送しているデータの長さ、あるいはデータが指定しているパラメータの組み合わせが、そのデータを処理するアプリケーションに誤動作を引き起こすとして予め設定された既知の条件を満たしているか否かが判定される（図11ステップS13）。

【0160】ここで上記条件を満たしていれば当該受信パケットは破棄の対象となる（図11ステップS15）。

一方、上記条件を満たしていなければ、当該受信

4に当該受信パケットの転送指示を行う（図11ステップS14）。

【0161】また、上記ステップS12に於いて、他のパケットの情報も必要であると判断された際は、断片化されたパケットで、かつ送出済みパケット保持機構76から取り出した他の断片化されたパケットとデータ領域がオーバーラップしている等、サーバに誤動作を引き起こすとして予め設定された既知の条件を満たしているか否かが判定される（図12ステップS21）。

【0162】ここで上記条件を満たしていれば当該受信パケットは破棄の対象となる（図12ステップS26）。一方、上記条件を満たしていなければ、次に、TCPのパケットで、送出済みパケット保持機構76から取り出した同一セッションの他のパケットとデータ領域がオーバーラップしている等、サーバに誤動作を引き起こすとして予め設定された既知の条件を満たしているか否かが判定される（図12ステップS22）。

【0163】ここで上記条件を満たしていれば当該受信パケットは破棄の対象となる（図12ステップS26）。一方、上記条件を満たしていなければ、送出済みパケット保持機構76から必要に応じた数の同一セッションのパケットを取り出し、送出に充分な長さのデータストリームを再構築し（図12ステップS23）、当該TCPデータストリームによって搬送されているデータの長さ、あるいはデータが指定しているパラメータは誤動作を引き起こすとして予め設定された既知の条件を満たしているか否かが判定される（図12ステップS24）。

【0164】ここで上記条件を満たしていれば当該受信パケットは破棄の対象となる（図12ステップS26）。一方、上記条件を満たしていなければ、パケット送出部74に当該受信パケットの転送指示を行う（図12ステップS25）。

【0165】このような不正アクセスに関わるパケットの判定処理が、パケット受信部71で受信した各受信パケットについて順次実行される。

【0166】上記したような不正アクセスに関わるパケットを排除する機能をもつことにより、宛先/送信元MACアドレスや、さらに上位のプロトコルの宛先/送信元アドレスやサービス番号等によってパケットを転送するか否かを判断するだけでは防止できない、不正アクセスに関わるパケットを通過させないパケット転送機構が実現できる。またパケットを転送するか否かの判断を行なうための設定を利用者が行なうことなく不正アクセスに関わるパケットを通過させないパケット転送機構を実現できる。またIPアドレス等のネットワークアドレスを全く持たないため、自身が不正アクセスの対象となることを防げる、不正アクセスに関わるパケットを通過させないパケット転送機構が実現できる。

される実行プログラム（パケット送出プログラム）は、例えばハードディスク、CD-ROM、半導体メモリ等の各種記憶媒体または記憶装置により提供することも可能である。

【0168】次に、図13を参照して本発明の第8実施形態を説明する。

【0169】図13は、本発明の第8実施形態によるパケット転送装置の要部の構成要素を示すブロック図である。

【0170】この図13に示す第7実施形態のパケット転送装置80は、シリアルインタフェース87を介してパケット解析プログラムを更新する機能を付加したことを特徴とする。

【0171】図13に示すパケット転送装置80に於いて、パケット解析機構85の実行命令格納部86には、命令実行機構（図10を参照）が動作するための実行プログラムが格納されている。

【0172】シリアルインタフェース87は、外部からの解析プログラム更新指示を受信する機能を持つ。解析プログラム更新機構88は、シリアルインタフェース87が受信した解析プログラム更新指示に従って、パケット解析機構85に格納された実行プログラムを更新する機能を持つ。更新指示形式識別機構89は、シリアルインタフェース87で受信したデータが、解析プログラム更新指示であるか否かを、当該受信したデータが特定の形式を満たしているか否かによって判定する機能を持つ。

【0173】上記図13に示すパケット転送装置80の動作を説明する。

【0174】シリアルインタフェース87を介して受信されたデータは解析プログラム更新機構88に渡される。解析プログラム更新機構88は、更新指示形式識別機構89によって、シリアルインタフェース87から渡されたデータが特定の形式を満たしている解析プログラム更新指示であることを確認すると、当該解析プログラム更新指示に含まれている実行プログラムを取り出す。

【0175】更に、解析プログラム更新機構88は、パケット解析機構85の命令実行機構が動作中か否かを確認し、動作中の場合は、動作が停止するのを待つ。パケット解析機構85の命令実行機構が停止していることを確認した場合、解析プログラム更新指示に含まれる実行プログラムをパケット解析機構85の実行命令格納部86に格納する。これにより、パケット解析機構85内の不正アクセスを解析する実行プログラムが更新される。

【0176】次に、図14を参照して本発明の第9実施形態を説明する。

【0177】図14は、本発明の第9実施形態によるパケット転送装置の要部の構成要素を示すブロック図である。

転送装置 90 は、ネットワークインタフェース 97 を介してパケット解析プログラムを更新する機能を付加したことを特徴とする。この第 9 の実施形態は、図 13 の実施形態のシリアルインタフェース 87 がネットワークインタフェース 97 に置き換わったものであり、その他の構成は図 13 と同じであるためその説明は省略する。

【0179】次に、図 14 に示すパケット転送装置 90 の動作を説明する。

【0180】ネットワークインタフェース 97 を介して受信されたデータは解析プログラム更新機構 98 に渡される。解析プログラム更新機構 98 は、更新指示形式識別機構 99 によって、ネットワークインタフェース 97 から渡されたデータが特定の形式を満たしている解析プログラム更新指示であることを確認すると、当該解析プログラム更新指示に含まれている実行プログラムを取り出す。

【0181】更に、解析プログラム更新機構 98 は、パケット解析機構 95 の命令実行機構が動作中か否かを確認し、動作中の場合は、動作が停止するのを待つ。パケット解析機構 95 の命令実行機構が停止していることを確認した場合、解析プログラム更新指示に含まれる実行プログラムをパケット解析機構 95 の実行命令格納部 96 に格納する。これにより、パケット解析機構 95 内の不正アクセスを解析する実行プログラムが更新される。

【0182】次に、図 15 を参照して本発明の第 10 実施形態を説明する。

【0183】図 15 は、本発明の第 10 実施形態によるパケット転送装置の要部の構成要素を示すブロック図である。

【0184】この図 15 に示す第 10 実施形態のパケット転送装置 100 は、パケットを利用して実行プログラム（パケット解析プログラム）を更新する機能を付加したことを特徴とする。

【0185】図 15 に示すパケット転送装置 100 に於いて、パケット解析機構 105 の実行命令格納部 106 には、命令実行機構（図 10 を参照）が動作するための実行プログラムが格納されている。

【0186】解析プログラム更新機構 107 は、パケット受信部 101 によって受信された解析プログラム更新指示に従って、パケット解析機構 105 に格納された実行プログラムを更新する機能を持つ。解析プログラム更新機構 107 内の更新指示形式識別機構 108 は、入力されたパケットのデータが特定の形式を満たしているか否かによって、受信パケットが解析プログラム更新指示であるか否かを判定する機能を持つ。

【0187】次に、図 15 に示すパケット転送装置 100 の動作を説明する。

【0188】パケット受信部 101 で受信されたパケットは、パケット識別付加機構 102 に渡される。この

プログラム更新機構 107 の更新指示形式識別機構 108 は、入力された受信パケットが解析プログラム更新指示を示す特定の形式を満たしていることを判定する。特定の形式を満たしている場合、その受信パケットは転送されるべきパケットではなく、解析プログラム更新指示であると判断する。これにより、解析プログラム更新機構 107 は当該受信パケットに含まれる実行プログラムを取り出して、パケット解析機構 105 に送り、実行命令格納部 106 に格納される。

【0189】上記した図 13 乃至図 15 に示す各実施形態は、何れもパケット解析機構の実行命令格納部に格納される実行プログラムを更新して、最新の不正アクセス解析プログラムが稼動する環境を整えるものであるが、不正な解析プログラム更新指示によって、不正アクセス解析プログラムが不正に更新されてしまい、パケット解析機構が正常に動作しないようにされてしまう可能性がある。

【0190】これを防ぐために、図 16 に示すように、更新指示形式識別機構に、電子署名識別機構を備え、解析プログラム更新指示に、電子署名を付加して認証することも可能である。尚、ここでは図 15 に示す第 10 実施形態を対象にしているが、図 13 に示す第 8 実施形態、図 14 に示す第 9 実施形態に於いても同様に適用可能である。

【0191】図 16 は、解析プログラム更新機構 107 の構成を示すブロック図であり、ここでは、解析プログラム更新機構 107 内に更新指示形式識別機構 108 と、更新指示形式識別機構 108 内に電子署名識別機構 109 を備える構成としている。

【0192】即ち、更新指示形式識別機構 108 内の電子署名識別機構 109 は、シリアルインタフェース（図 13）や、ネットワークインタフェース（図 14）から受信したデータや、パケット受信部（図 15）で受信されたパケットに格納されているデータ中に含まれている電子署名が正当な署名であるか否かを判定する。即ち、解析プログラム更新指示を示すデータが、特定の形式を満たしており、かつ当該データ中に含まれている電子署名が正当な署名である場合に、正当な解析プログラム更新指示であると判定する。

【0193】解析プログラム更新機構 107 は、更新指示形式識別機構 108 が、正当な解析プログラム更新指示であると判定した場合、その解析プログラム更新指示に含まれる不正アクセス解析プログラムをパケット解析機構 105 に出力する機能を有する。

【0194】上記の構成において、解析プログラム更新機構 107 に渡されたデータが、解析プログラム更新指示であることを示す特定の形式を満たしており、かつ、電子署名識別機構 109 によって当該データ中に含まれている電子署名が正当な署名である場合、解析プログラ

ると判定し、そのデータに含まれる不正アクセス解析プログラムを取り出して、パケット解析機構 105 に送り、パケット解析機構 105 は実行命令格納部 106 に不正アクセス解析プログラムを格納する。これにより、不正な解析プログラム更新指示によって、パケット解析機構が正常に動作しないようにされてしまうことを防げるパケット転送装置を実現することができる。

【0195】次に、図 17 を参照して本発明の第 11 実施形態を説明する。

【0196】図 17 は、本発明の第 11 実施形態によるパケット転送装置の要部の構成要素を示すブロック図である。この第 11 実施形態のパケット転送装置 110 は、通信用アドレスを予め設定する機能をもつことを特徴とする。

【0197】図 17 に示すパケット転送装置 110 に於いて、通信用アドレス設定機構 114 は、シリアルインタフェースやネットワークインタフェース等を介して得られる通信用アドレスを、通信用アドレス保持機構 115 に設定する機能を持つ。この図 17 に示す例では、シリアルインタフェース 113 を介して通信用アドレスを設定する場合を例に示している。

【0198】通信用アドレス保持機構 115 は、通信用アドレス設定機構 114 によって予め設定された通信用アドレスを保持する機能を持つ。

【0199】通信制御機構 112 は、パケット解析プログラムの更新に伴う通信や、装置内情報通知機構 117 がネットワークセグメントに接続される他の装置に対して通知するための通信（以下、これらの通信を特定通信と称する）を制御する装置であり、上記特定通信を行なわないときは、上記通信アドレス宛のパケットは破棄する機能を持つ。また、上記特定通信を行なうときには、上記通信アドレス宛のパケットを受信し、当該パケットに格納された当該特定通信に関わるデータを実行プログラム更新機構 116 や装置内情報通知機構 117 へ渡す機能を持つ。また、上記特定通信に関わるデータ通信時に、実行プログラム更新機構 116 や装置内情報通知機構 117 が送信するデータに当該通信アドレスを送信元として付加してネットワークセグメントへ送出する機能を持つ。

【0200】この実施形態のパケット転送装置 110 には、例えば、図 6 に示す不正アクセス履歴保持機構 66 に保持されている不正アクセス履歴や、その他の装置内部の情報を外部に通知するための装置内情報通知機構 117 を持たせている。装置内情報通知機構 117 は、装置内部の情報を外部へ通知するのに、シリアルインタフェースや、通知用ネットワークインタフェースを利用する。また、装置内情報通知機構 117 は、装置内部の情報を外部に通知するのに、パケット転送の対象である、パケ...

自身が不正アクセスの対象となることを防ぐために通常動作中は持っていない、ネットワークアドレスが必要となる。

【0201】次に、図 17 に示すパケット転送装置 110 の動作を説明する。

【0202】利用者は、通信用アドレス設定機構 114 を利用して、通信用アドレス保持機構 115 に、通信用アドレスを予め設定しておく。図 17 の構成では、シリアルインタフェース 113 を介して通信用アドレス設定機構 114 を利用する場合を示しているが、ネットワークインタフェースを利用したり、解析プログラム更新指示と同様の方法で、転送対象のネットワークセグメントを介して、通信用アドレス設定機構 114 を利用することも可能である。

【0203】上記特定通信を行なう場合、通信制御機構 112 は、ネットワークセグメントからパケット受信部 111 を介して当該通信アドレス宛のパケットが送信されてきた場合、これを受信し、その受信パケットに含まれる通信に関わるデータを実行プログラム更新機構 116 や装置内情報通知機構 117 へ渡す。そして、実行プログラム更新機構 116 や装置内情報通知機構 117 は特定通信に関わる送信データを、上記通信アドレス宛によって示される送信元のネットワークセグメントへ送出する。しかしながら、通信を行なわないときは、通信制御機構 112 が上記通信アドレス宛のパケットを破棄し、自身が不正アクセスの対象となることを防ぐ。

【0204】次に、図 18 および図 19 を参照して本発明の第 12 実施形態を説明する。

【0205】図 18 は、本発明の第 12 実施形態によるパケット転送装置の要部の構成要素を示すブロック図である。この図 18 に示す第 12 実施形態のパケット転送装置 120 は、パケット横奪部 122 を持つ構成としたことを特徴とする。

【0206】図 18 に示すパケット転送装置 120 に於いて、通信用アドレス選択機構 124 は、過去に受信したパケットのネットワークアドレスと受信したネットワークセグメントとの対応を保持するアドレス／セグメント対応表 125 を持ち、上記特定通信に関わるパケットの送出先ネットワークセグメントとは異なるネットワークセグメントから、過去に受信したパケットの送信元アドレスのうちの任意の 1 つを通信用アドレスとして選択し、その選択した通信用アドレスを通信用アドレス保持機構 126 に設定する機能を持つ。

【0207】この際のアドレス／セグメント対応表 125 の一例を図 19 に示している。

【0208】通信用アドレス保持機構 126 は、通信用アドレス選択機構 124 によって設定された通信用アドレスを保持する機能を持つ。

【0209】パケ...

ト識別子付加機構（図 1 乃至図 6 を参照）に渡して、通常の転送処理を行ない、上記特定通信を行なうときは通信アドレス宛のパケットをパケット識別子付加機構に渡さずに横奪する機能を持つ。

【0210】通信制御機構 123 は、上記特定通信を制御する機構であり、受信パケットに含まれる通信に関わるデータを実行プログラム更新機構 127 や、装置内情報通知機構 128 へ渡す。また、実行プログラム更新機構 127 や装置内情報通知機構 128 が送信するデータに、当該通信アドレスを送信元として付加してネットワークセグメントへ送出する機能を持つ。

【0211】次に、図 18 に示すパケット転送装置 120 の動作を説明する。

【0212】通信用アドレス選択機構 124 は、内蔵するアドレス／セグメント対応表 125 を参照して、特定通信に関わるパケットの送出先となるネットワークセグメントから、過去に受信したパケットの送信元アドレスの 1 つを通信用アドレスとして選択する。

【0213】ここで、アドレス／セグメント対応表 125 に保持された、アドレスと受信したネットワークセグメントの対応が、例えば図 19 に示す内容であるとする。ここで、上記特定通信を行なう相手が、[192. 168. 7. 42] のネットワークアドレスを持っているとすると、上記特定通信に関わるパケットを送出すべきネットワークセグメントはセグメント B であることが判る。

【0214】したがって、上記特定通信に関わるパケットを送出すべきネットワークセグメント（セグメント B）と異なるネットワークセグメントとはセグメント A であり、通信用アドレスとしては、[192. 168. 0. 21]、あるいは [192. 168. 3. 134] のいずれかを選択すれば良いこととなる。

【0215】例えば、アドレス／セグメント対応表 125 の先頭に最も近いセグメント A を選択するとすると、アドレスは [192. 168. 0. 21] となる。この際、もしも、上記特定通信を行なう相手のネットワークアドレスが、アドレス／セグメント対応表 125 に存在しなかった場合は、各々のネットワークセグメント上のアドレスを任意に選択し、そのアドレスを用いてアドレス設定を行う。このアドレス設定の結果、いずれかのネットワークセグメント上で、アドレス設定の応答パケットを受信できると、アドレス／セグメント対応表 125 に当該通信を行なう相手のネットワークアドレスとネットワークセグメントが登録されるので、改めて当該ネットワークアドレスを通信用アドレスとして選択する。

【0216】通信用アドレスをこのように選択することで、当該通信アドレスが指定されている応答パケットがパケット転送装置 120 のパケット受信部 121 に送信

トは、パケット識別子付加機構に渡して通常の転送処理を行なう。一方、上記特定通信を行なうときは、セグメント A の通信アドレス宛のパケットを横奪して、当該通信用アドレスの本来の持ち主にパケットが渡らないようにする。

【0217】パケット横奪部 122 は、通信制御機構 123 が送出したパケットに対するネットワークセグメントからの応答パケットのみを横奪することで、当該通信用アドレスの本来の持ち主の通信への影響を最小限にすることも可能である。この場合、当該通信用アドレスの本来の持ち主の通信と区別ができるように、当該通信用アドレスの本来の持ち主が、この実施形態によるパケット転送装置 120 を経由する通信で用いているポート番号等を保存しておき、当該装置の通信時は、それらと重ならないようにして当該通信用アドレスの本来の持ち主の通信と区別できるようにする等の仕組みを用意する必要がある。このようにすることで、自身への不正アクセスを防ぎつつ、解析プログラムの更新に伴う通信や、装置内情報通知機構が他の装置に対して装置内部の情報を通知するための特定通信が可能となる。

【0218】上記した図 17、若しくは図 18 に示した各実施形態の構造をもつことによって、解析プログラムの更新に伴う通信や、装置内情報通知機構が他の装置に対して装置内部の情報を通知するための通信、等の特定の通信を行なっているとき以外は、ネットワークアドレスを持たないため、自身への不正アクセスを防げるパケット転送装置を実現することができる。

【0219】次に、図 20 および図 21 を参照して本発明の第 13 実施形態を説明する。

【0220】図 20 は、本発明の第 13 実施形態によるパケット転送装置の要部の構成要素を示すブロック図である。この図 20 に示す第 13 実施形態のパケット転送装置 130 は、通信開始指示形式識別機構 133 を具備することを特徴とする。

【0221】通信開始指示形式識別機構 133 は、パケット受信部 131 で受信されたパケットが、通信開始指示を示す特定の形式を満たしているデータであることを識別して、通信制御機構 134 に通信開始を通知する機能を持つ。

【0222】通信制御機構 134 は、通信開始指示形式識別機構 133 からの通信開始の通知を受けると、通信用アドレス保持機構 136 に保持された通信用アドレス、あるいは通信用アドレス選択機構 135 が選択した通信用アドレスを用いた通信を開始する機能を持つ。

【0223】次に、図 20 に示すパケット転送装置 130 の動作を説明する。

【0224】上記した図 17 および図 18 に示す各実施形態の構造によって、上記特定通信を行なっているとき

から他の装置に対して通信を開始することが可能であるが、他の装置から上記実施形態のパケット転送装置へ対する通信を開始しようとしても、ネットワークアドレスを持たないため、通信が不可能である。そこで、この図20に示す第13実施形態のパケット転送装置130では、他の装置からパケット転送装置130に対する通信を開始することができるようにするため、通信開始指示形式識別機構133を持つ。

【0225】パケット受信部131で受信されたパケットは、パケット識別子付加機構(図1乃至図6など参照)等に渡されるのと同時に、通信開始指示形式識別機構133にも渡される。通信開始指示形式識別機構133は、受信したパケットの形式が、通信開始指示を示す特定の形式を満たしているか否かを判定する。

【0226】特定の形式を満たしている場合、受信したパケットは、ネットワークセグメントに送出されるべきパケットではなく、パケット転送装置130に対する通信開始指示であると判断し、通信制御機構134は通信開始を指示する。この図20に示す例では、通信制御機構134が通信用アドレス選択機構135で選択した通信用アドレスを用いて通信を開始すると想定する。

【0227】このようにすることで、解析プログラムの更新に伴う通信や、装置内情報通知機構138が他の装置に対して装置内部の情報を通知するための通信、等なる特定通信を行なっているとき以外は、パケット転送装置130はネットワークアドレスを持たないため、自身への不正アクセスを防ぐことができ、かつ他の装置からパケット転送装置130に対する通信を開始することが可能なパケット転送機能を実現することができる。

【0228】上記した実施形態に於いては、外部から通信を開始する機能を持つ場合、不正な通信開始指示によって通信を開始され、自身が不正アクセスの対象とされてしまう可能性がある。これを防ぐために、図21に示すように、通信開始指示形式識別機構133に、電子署名識別機構139を備え、通信開始指示に、電子署名を付加して認証することも可能である。

【0229】図21に示すように、通信開始指示形式識別機構133内には電子署名識別機構139が設けられ、この電子署名識別機構139は通信開始指示のデータ中に含まれている電子署名が正当な署名であるか否かを判定して、電子署名が正当な署名である場合に、当該データは正当な通信開始指示であると判定し、通信制御機構134に通信開始を通知する。

【0230】通信制御機構134は、通信開始指示形式識別機構133から通信開始の通知を受けると、通信用アドレス保持機構136に保持された通信用アドレス、あるいは通信用アドレス選択機構135が選択した通信用アドレスを用いた通信を開始する。

【0231】これにより、不正な通信開始指示によ

てしまうことを防げるパケット転送装置を実現することができる。

【0232】尚、上記した図13乃至図20に示す各実施形態に於いて扱われるパケット解析プログラムは、例えばハードディスク、CD-ROM、半導体メモリ等の各種記憶媒体または記憶装置により装置個々に個別に提供することも可能である。

【0233】上記したような本発明の実施形態により、宛先/送信元MACアドレスや、さらに上位のプロトコルの宛先/送信元アドレスやサービス番号等によってパケットを転送するか否かを判断するだけでは防止できない、不正アクセスに関わるパケットを通過させないパケット転送装置を実現することができる。また、パケットを転送するか否かの判断を行なうための設定を利用者が行なうことなく、不正アクセスに関わるパケットを通過させないパケット転送装置を実現することができる。また、IPアドレス等のネットワークアドレスを全く持たないため、自身が不正アクセスの対象となることを防げる、不正アクセスに関わるパケットを通過させないパケット転送装置を実現することができる。また、不正アクセスが為されていることを表示可能なパケット転送装置を実現することができる。

【0234】更に、上記した実施形態の機能を、図22乃至図24を参照して説明した既存の不正アクセス防止機能と組み合わせることで、より信頼性の高い不正アクセスに関わるパケットの転送防止機能を実現することができる。

【0235】

【発明の効果】以上詳記したように本発明によれば、利用者に大きな作業負担をかけることなく、信頼性の高い不正アクセスの防止機能を実現できる。更に本発明によれば、送信元より転送されたパケットの内容を送出して不正アクセスに関わるパケットでないことを判定する機能をもつことで、不正アクセスに関わるパケットの転送を確実に防止でき、信頼性の高い不正アクセスの防止機能が実現できる。即ち本発明によれば、宛先/送信元MACアドレスや、さらに上位のプロトコルの宛先/送信元アドレスやサービス番号等によってパケットを転送するか否かを判断するだけでは防止できない、不正アクセスに関わるパケットを通過させないパケット転送装置を実現することができる。またパケットを転送するか否かの判断を行なうための設定を利用者が行なうことなく不正アクセスに関わるパケットを通過させないパケット転送装置を実現することができる。またIPアドレス等のネットワークアドレスを全く持たないため、自身が不正アクセスの対象となることを防ぐことのできる、不正アクセスに関わるパケットを通過させないパケット転送装置を実現することができる。更に不正アクセスが為されていることを表示可能なパケット転送装置を実現する

【図面の簡単な説明】

【図1】本発明の第1実施形態によるパケット転送装置の要部の構成要素を示すブロック図。

【図2】本発明の第2実施形態によるパケット転送装置の要部の構成要素を示すブロック図。

【図3】本発明の第3実施形態によるパケット転送装置の要部の構成要素を示すブロック図。

【図4】本発明の第4実施形態によるパケット転送装置の要部の構成要素を示すブロック図。

【図5】本発明の第5実施形態によるパケット転送装置の要部の構成要素を示すブロック図。

【図6】本発明の第6実施形態によるパケット転送装置の要部の構成要素を示すブロック図。

【図7】上記第6実施形態に於ける不正アクセス表示手段の第1の例を示す図。

【図8】上記第6実施形態に於ける不正アクセス表示手段の第2の例を示す図。

【図9】本発明の第7実施形態によるパケット転送装置の要部の構成要素を示すブロック図。

【図10】上記第7実施形態に於けるパケット解析機構の構成例を示すブロック図。

【図11】上記第7実施形態に於ける不正アクセスに関わるパケットの判定処理の処理手順を示すフローチャート。

【図12】上記第7実施形態に於ける不正アクセスに関わるパケットの判定処理の処理手順を示すフローチャート。

【図13】本発明の第8実施形態によるパケット転送装置の要部の構成要素を示すブロック図。

【図14】本発明の第9実施形態によるパケット転送装置の要部の構成要素を示すブロック図。

【図15】本発明の第10実施形態によるパケット転送装置の要部の構成要素を示すブロック図。

【図16】上記第10実施形態に於ける解析プログラム更新機構の構成を示すブロック図。

【図17】本発明の第11実施形態によるパケット転送装置の要部の構成要素を示すブロック図。

【図18】本発明の第12実施形態によるパケット転送装置の要部の構成要素を示すブロック図。

【図19】上記第12実施形態に於けるアドレス/セグメント対応表の構成例を示す図。

【図20】本発明の第13実施形態によるパケット転送装置の要部の構成要素を示すブロック図。

【図21】上記第13実施形態に於ける通信開始識別機構の他の構成例を示すブロック図。

【図22】従来のパケット転送装置の構成を示すブロック図。

【図23】上記図22に示す従来のパケット転送装置の

ネットワーク構成例を示すブロック図。

【図24】上記図23に示す従来のパケット転送装置のルール保持部に格納される内容例を示す図。

【符号の説明】

10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110, 120, 130…パケット転送装置

11, 21a, 21b, 31a, 31b, 41, 51, 61, 71, 81, 91, 101, 111, 121, 131…パケット受信部

12, 22a, 22b, 32, 42, 52, 62, 72, 82, 92, 102…パケット識別子付加機構

13, 23a, 23b, 33, 43, 53a…53n, 63, 73, 83, 93, 103, …パケット保留キュー

14, 24a, 24b, 34a, 34b, 44a…44n, 54a…54n, 64, 74, 84, 94, 104, …パケット送出部

15, 25a, 25b, 35, 45, 55, 65, 75, 85, 95, 105…パケット解析機構

150, 250a, 250b, 350, 450, 550, 650…不正パケット解析用データベース

46, 56…送出セグメント判定機構

66…不正アクセス履歴保持機構

67…不正アクセス履歴表示機構

67A…不正アクセス表示器

67B…不正アクセス表示装置

76…送出済みパケット保持機構

86, 96, 106…実行命令格納部

87, 113…シリアルインタフェース

88, 98, 107…解析プログラム更新機構

89, 99, 108…更新指示形式識別機構

97…ネットワークインタフェース

109, 139…電子署名識別機構

112, 123, 134…通信制御機構

114…通信用アドレス設定機構

115, 126, 136…通信用アドレス保持機構

116, 127, 137…実行プログラム更新機構

117, 128, 138…装置内情報通知機構

122, 132…パケット横奪部

124, 135…通信用アドレス選択機構

125…アドレス/セグメント対応表

133…通信開始指示形式識別機構

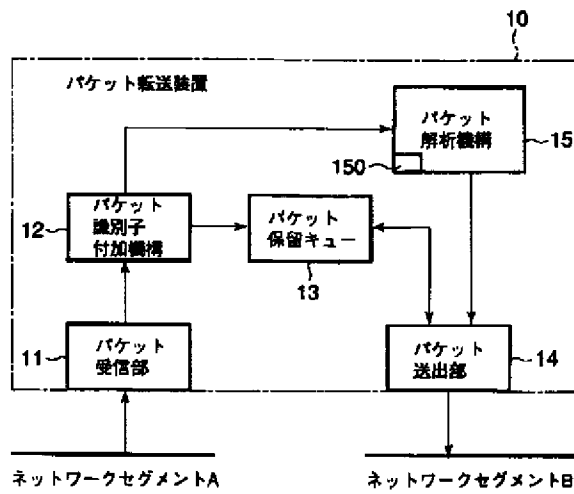
751…パケット格納部

752…実行命令格納部

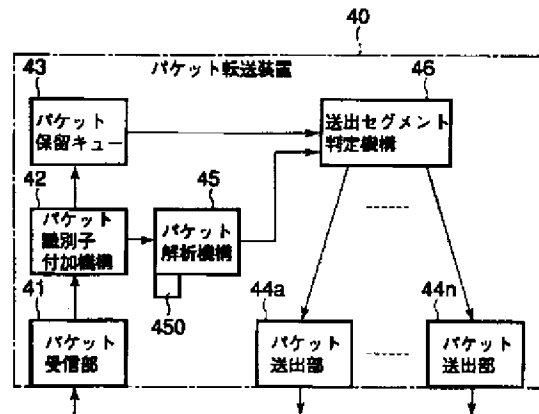
753…メモリ制御機構

754…命令実行機構

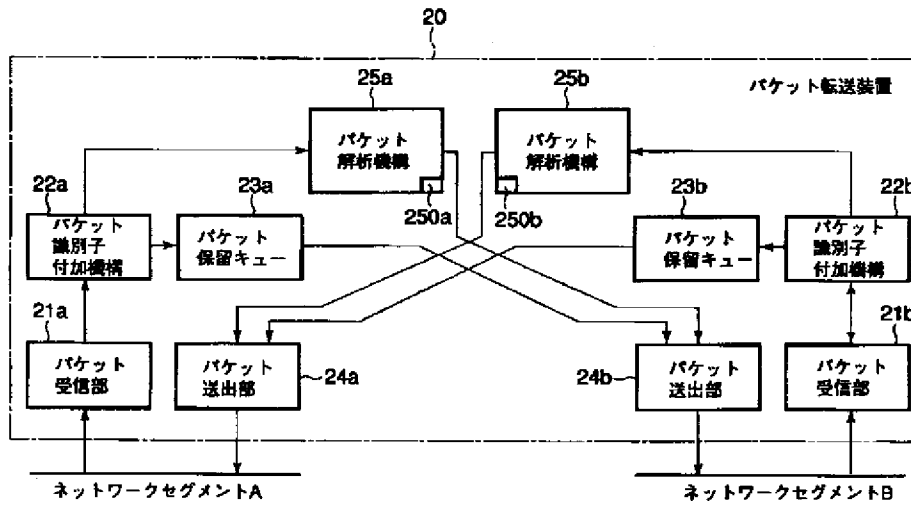
【図1】



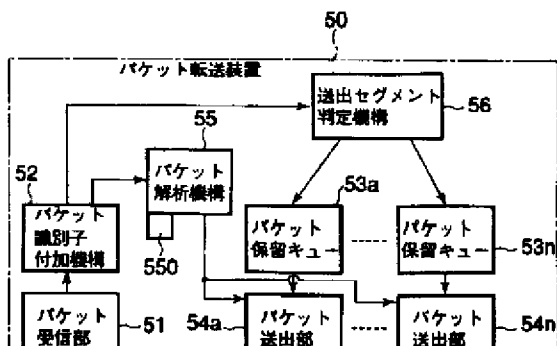
【図4】



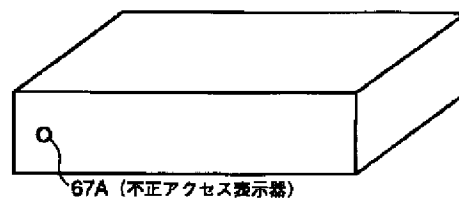
【図2】



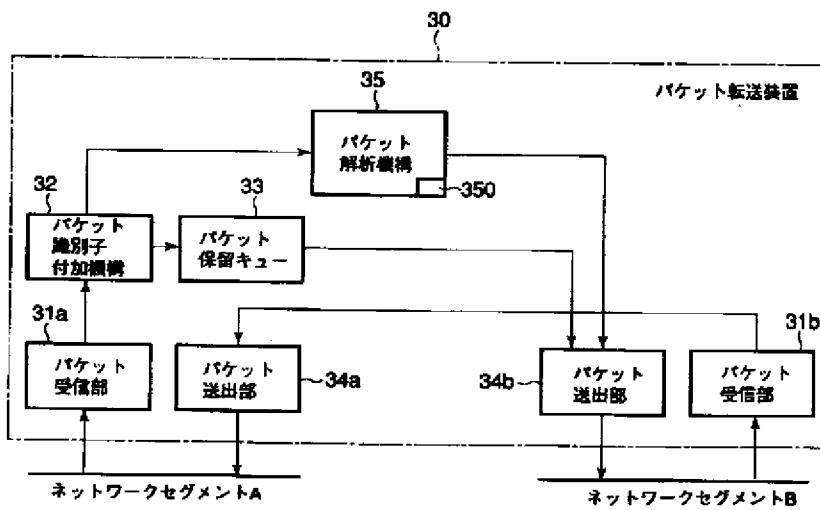
【図5】



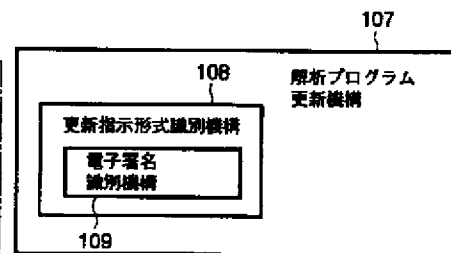
【図7】



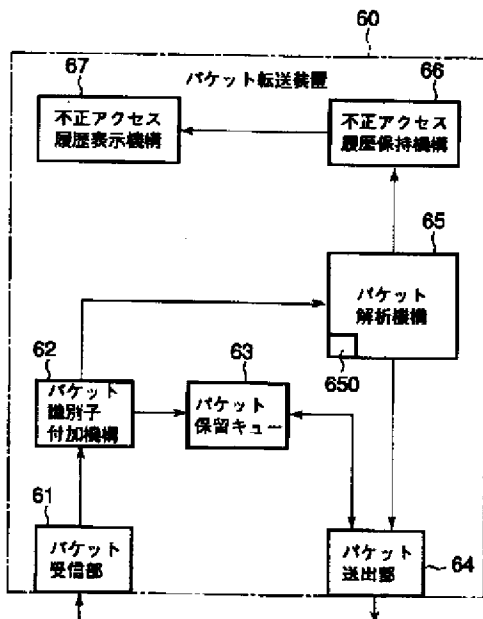
【図 3】



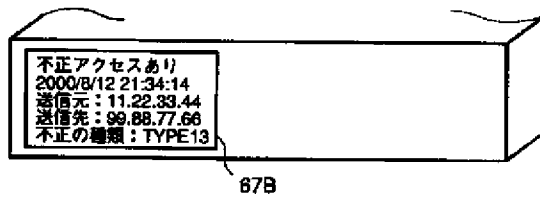
【图 16】



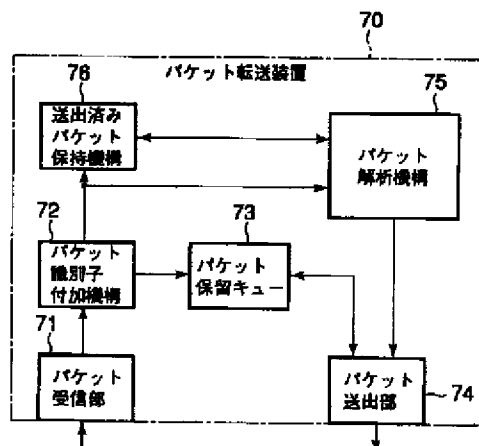
【※6】



【図 8】

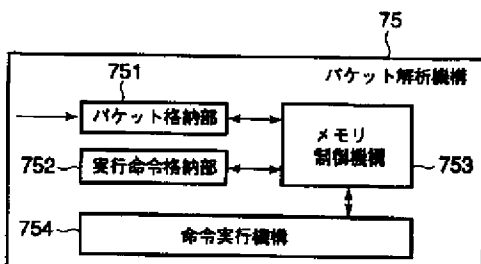


【図9】



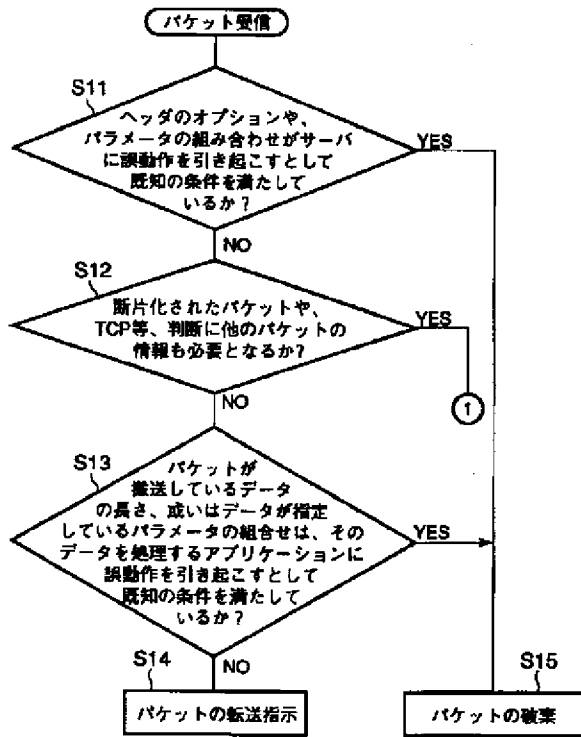
【図 10】

【图 19】

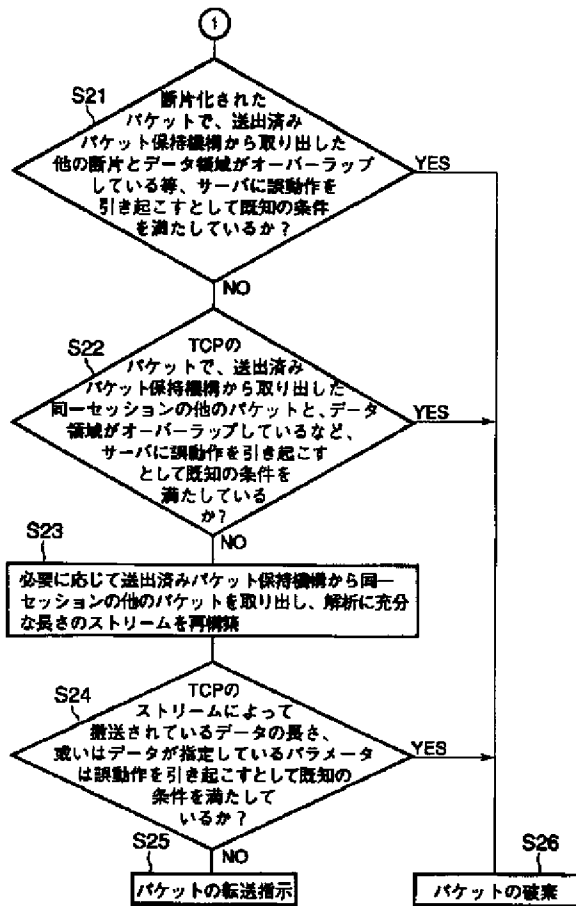


アドレス	受信したネットワークセグメント
192.168.0.21	セグメントA
192.168.1.17	セグメントB
192.168.1.232	セグメントB
192.168.3.134	セグメントA
192.168.7.42	セグメントB

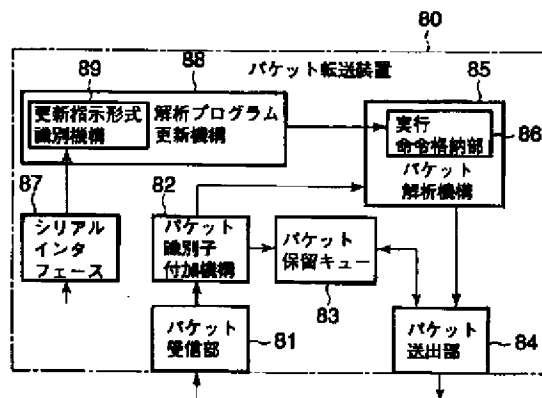
【図11】



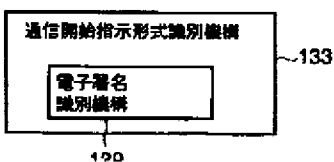
【図12】



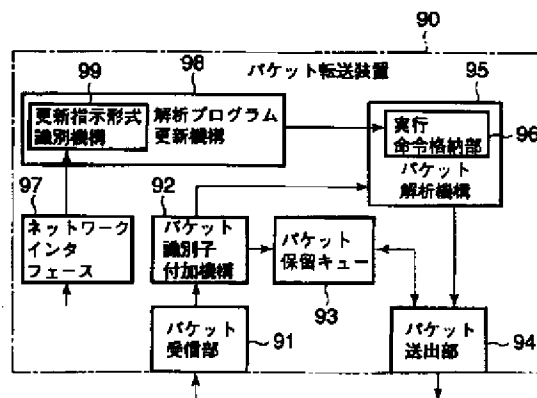
【図13】



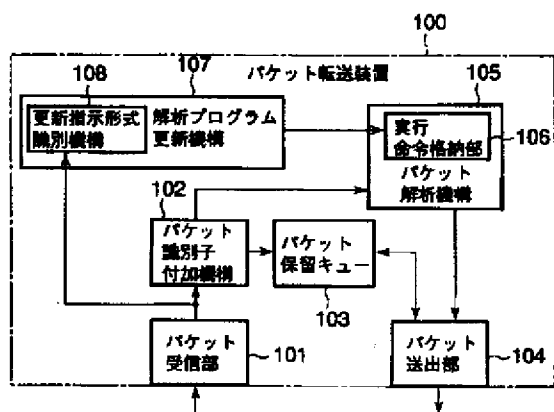
【図21】



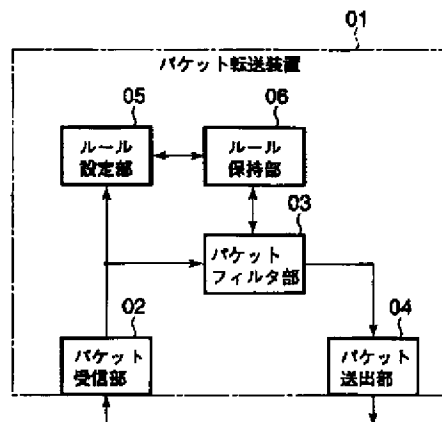
【図14】



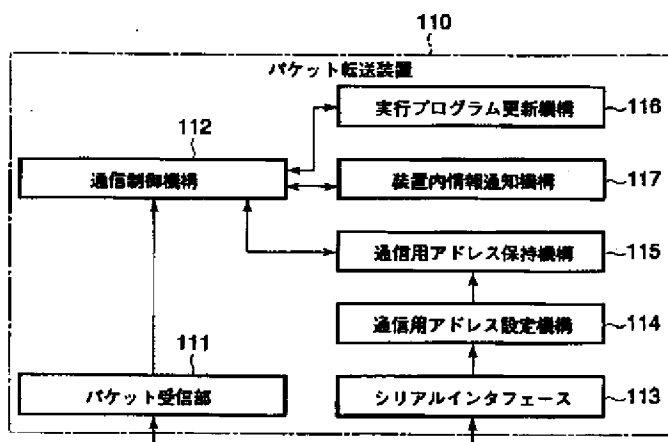
【図15】



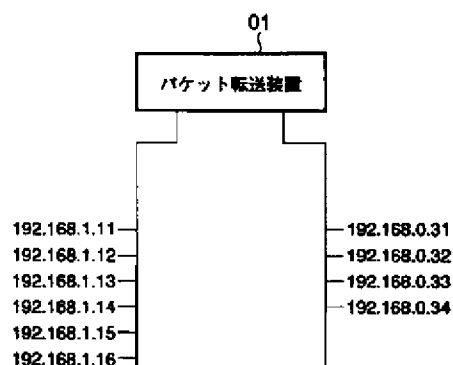
【図22】



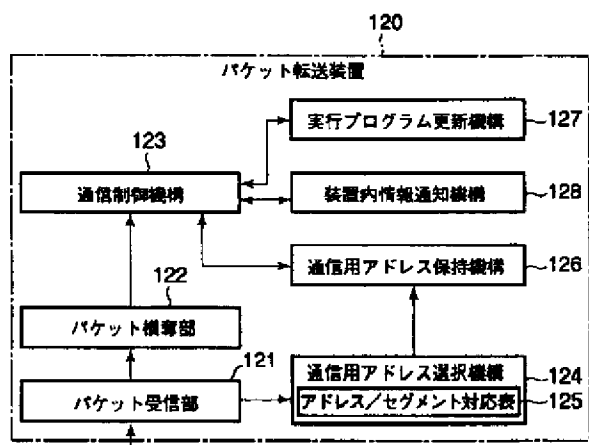
【図17】



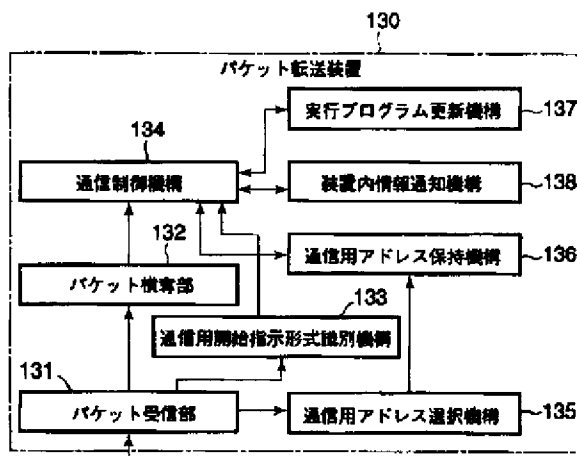
【図23】



【図18】



【図20】



【図24】

宛先	送信元	宛先	転送許可
192.168.0.31	192.168.1.11	HTTP	許可
192.168.0.31	192.168.1.12	HTTP	許可
192.168.0.31	192.168.1.13	HTTP	不許可
192.168.0.31	192.168.1.14	HTTP	不許可
192.168.0.31	192.168.1.11	SMTP	許可
192.168.0.31	192.168.1.12	SMTP	不許可
192.168.0.31	192.168.1.13	SMTP	不許可
192.168.0.31	192.168.1.14	SMTP	許可
192.168.0.33	any	HTTP	許可
any	192.168.1.15	HTTP	不許可
any	192.168.1.16	SMTP	許可